



---

## **Configuring a Converged User with the “Collaboration Pack for CS 1000” using Avaya Aura® Midsize Enterprise Solution Release 6.2 and Avaya Communication Server 1000 Release 7.5 – Issue 1.0**

### **Abstract**

This Application Note describes the detailed procedures for configuring a Converged User with the “Collaboration Pack for CS 1000”. This solution consists of the Avaya Communication Server 1000 Release 7.5 and the Avaya Aura® Midsize Enterprise solution Release 6.2. In the sample configuration described herein, a Converged User is defined as a user having a Communication Server 1000 client and a Collaboration Pack client sharing the same Directory Number such that simultaneous ring (SIMRING), a single Avaya CallPilot voicemail box and aggregated Presence are enabled for the user. The steps documented in this Application Note focus on how these attributes are configured across the solution.

Avaya Aura® Midsize Enterprise solution is virtualized to a single server which includes a flexible SIP-enabled communications platform, messaging, conferencing, centralized management and administration tools, and an application development interface. Each capability operates the same as when running on its own server. Communication Server 1000 is a telephony application server used here to provide the Converged User capability. A narrow set of client endpoints as well as capabilities of the Avaya Aura® solution were tested in this sample configuration.

## Table of Contents:

1. Introduction.....	4
2. General Test Approach and Test Results.....	5
2.1. Interoperability Compliance Testing.....	5
2.2. Test Results and Observations .....	6
3. Reference Configuration.....	7
3.1 Avaya Aura® Midsize Enterprise Solution Components .....	7
3. Equipment and Software Validated .....	9
4. Configure Avaya Communication Server 1000E .....	10
4.1. Enable UCM Services in SMGR.....	10
4.2. Confirm Node and IP Addresses.....	12
4.3. Confirm Virtual D-Channel, Routes and Trunks .....	14
4.3.1. Confirm Virtual D-Channel Configuration.....	14
4.3.2. Confirm Routes and Trunks Configuration .....	14
4.4. Configure SIP Trunk to Avaya Aura® Session Manager .....	16
4.5. Configure ESN for Route List Index and Digit Manipulation .....	19
4.6. Configure Avaya Communication Server 1000 Presence Services .....	23
4.6.1. TLS & Certificates section.....	23
4.6.2. Change Session Manager Access Point Address:.....	25
4.6.3. Verify Communication Server 1000 UCM Security Certificates:.....	27
4.6.4. Communication Server 1000 Presence User Agent Configuration: .....	28
4.6.5. Configure Presence Publisher to Session Manager .....	31
4.6.6. Configure Presence Services for all Communication Server 1000 Users.....	34
4.7. Save Configuration.....	36
5. Configure Avaya Aura® Session Manager .....	38
5.1. Verify SIP Domains .....	39
5.2. Define Location for Avaya Communication Server 1000 .....	39
5.3. Configure Adaptation Module .....	40
5.4. Define SIP Entities .....	42
5.5. Define Entity Links .....	44
5.5.1. Entity Links Communication Server 1000 .....	44
5.5.2. Entity Link for Communication Manager.....	45
5.6. Define Routing Policy .....	46
5.7. Define Dial Pattern.....	47
6. Configure Avaya Aura® Communication Manager.....	50
6.1. Verify System Access Codes match.....	50
6.2. Verify IP Network Region - Domain .....	53

6.3.	Configure Trunk-to-Trunk Transfers .....	54
6.4.	Administer Signal Group .....	56
6.5.	Administer SIP Trunk Group .....	57
6.6.	Verify Signal Group and Trunk Group are In-Service.....	58
6.7.	Configure Incoming Call Handling for Trunk Group .....	59
6.8.	Verify IP Network Region - Domain .....	60
6.9.	Administer Private Numbering Plan (.....	61
6.10.	Administer Public Numbering Plan.....	62
6.11.	Administer Uniform Dial Plan .....	63
6.12.	Administer Route Pattern .....	64
6.13.	Administer ARS Analysis .....	65
6.14.	Administer ARS Digit Conversion.....	66
7.	Avaya Aura® Presence Services Configuration.....	68
7.1.	Verify Configuration of Trusted Hosts .....	68
7.2.	Verify Configuration to support Avaya SIP Endpoints .....	71
8.	Configure CallPilot .....	73
8.1.	Registering CallPilot to the Element Registry .....	73
8.2.	Adding CallPilot certificate to System Manager.....	74
9.	User Management .....	77
9.1.	Create User Identities and Communication Profiles in System Manager.....	77
	Select the Commit & Continue button (not shown).....	84
9.2.	Synchronize Communication Profiles.....	84
9.2.1.	Communication Server 1000 .....	84
9.2.2.	CallPilot .....	86
9.3.	Multiple Message Waiting Indication (MWI) for Collaboration .....	86
9.4.	Personal Call Assistant Configuration (PCA).....	88
9.5.	Manual Configuration of Avaya SIP Clients .....	90
9.5.1.	Avaya Flare® Communicator on iPad.....	90
9.5.2.	Avaya one-X Mobile SIP for iOS on iPhone.....	92
10.	Verification Steps.....	95
10.1.	Verify Operational Status .....	95
10.1.1.	Verify Avaya Aura® Session Manager Operational Status.....	95
10.1.2.	Verify SIP Entity Link Status.....	96
10.1.3.	Verify Registrations of SIP Endpoints .....	96
11.	Conclusion .....	98
12.	Additional References.....	99
13.	Change History .....	100

# 1. Introduction

This Application Note describes the procedures for configuring the “Collaboration Pack for CS 1000” with Avaya Aura® Mid Size Enterprise solution Release 6.2 and Avaya Communication Server 1000 Release 7.5.

“Collaboration Pack for CS 1000” offer is based on Avaya Aura® Midsize Enterprise Release 6.2 and is used to accelerate the introduction of new collaboration clients to the Communication Server 1000 installed base. In this initial offer the collaboration clients tested are Avaya SIP clients Flare Communicator for iPad and one-X Mobile (SIP) for iOS. Additional clients and capabilities will be added to “Collaboration Pack for CS 1000” over time.

The notion of a “Converged User” is introduced with the “Collaboration Pack for CS 1000”. A Converged User is defined as a user having both a traditional Communication Server 1000 client “twinned” with a collaboration client (such as an Avaya Flare Communicator or one-X Mobile SIP client). These two endpoints are seen by other users to be associated with a single user. They also share a single number for incoming and outgoing calls, single voicemail box via CallPilot and a single aggregated presence.

Avaya Aura® Midsize Enterprise 6.2 currently supports up to 1,000 users on a single server platform that includes virtualized instances of Avaya Aura® Session Manager, Avaya Aura® System Manager, Avaya Aura® Communication Manager and Avaya Aura® Presence Services. A G430 or G450 gateway is also included as standard with the Avaya Aura® Midsize Enterprise 6.2.

The Avaya Communication Server 1000 R7.5 is used to provide advanced telephony capability to the Converged User via M3900 series digital sets or 1100 / 1200 series IP sets with UNISTim software. PSTN trunks (SIP or ISDN) are also accessed via the Avaya Communication Server 1000 R7.5. Collaboration Pack for CS 1000 is supported via SIP trunks to either CS 1000M or CS 1000E.

CallPilot 5.0 provides voice mail capability to the Converged User, single voicemail box and Message Waiting Indication (MWI). Network Message Service (NMS) capability must be enabled on CallPilot.

Throughout this Application Note the commercial offer, “Collaboration Pack for CS 1000” will be abbreviated and referred as “Collaboration Pack or Collab Pack”. Likewise, either an Avaya Flare Communicator on iPad or Avaya one-X Mobile SIP for iOS client will be referred to as “collaboration client or SIP client”.

**Please complete the following survey to provide feedback on this Application Note.**

<https://talktous.avaya.com/TakeSurvey.aspx?SurveyID=144J4n5>

## 2. General Test Approach and Test Results

A reference configuration containing all of the equipment for the Collaboration Pack for CS 1000 was installed at Avaya Test Labs. A number of tests cases were executed to ensure functionality of a Converged User and interoperability between the Communication Server 1000 and Avaya Aura® Mid Size Enterprise solution; aka the Collaboration Pack.

The two clients are “twinned” with one another via the Personal Call Assistant (PCA) feature on the Communication Server 1000. The PCA feature or “PCA call” provides simultaneous ringing (SIMRING) of the two clients in the case of an incoming call to the Communication Server 1000 client. The user can answer on either client, (Communication Server 1000 client or collaboration client on the Collaboration Pack) and the other will stop ringing. In the case of no answer or busy, call redirection will occur as defined for the Communication Server 1000 client – this could include redirection to a single CallPilot voice mailbox. In the case of an outgoing call from the Converged User, in the case of the Avaya SIP client on the Collaboration Pack, the Calling Line Identification (CLID) feature of Communication Manager is used to send the CLID associated with the Communication Server 1000 client to ensure single number identity. For presence aggregation the telephony presence of the Communication Server 1000 client is pushed to the Avaya Aura® Presence Services, which also receives/pushes presence updates for the collaboration client

PSTN calling is achieved via the Communication Server 1000 for all clients. This can be via ISDN or SIP trunks.

### 2.1. Interoperability Compliance Testing

To verify the interoperability and operation of a Converged User the following features and functionality were covered during the testing:

- Simultaneous ringing for inbound calls
- Single number for CLID on incoming and outgoing calls
- Single voicemail box via CallPilot
- MWI via CallPilot
- Voicemail navigation for inbound and outbound calls via CallPilot
- Aggregation of presence status across devices for a Converged User
- Incoming and outgoing PSTN calls
- Point to point calls (converged user to converged user)
- Multiple call scenarios
- User features such as hold and resume, transfer and conference
- Caller ID presentation during incoming and call transfers
- Proper codec negotiation (G711 and G729)
- E.164 dialing
- Presence status during basic call scenarios
- Call Detail Recording (CDR) on the Communication Sever 1000

The following was not tested with the Collaboration Pack for Communication Server 1000:

- Multiple Communication Server 1000

- High Availability, Geo-redundancy and Branch solutions
- 2,400 users capacity of the Avaya Mid Size Enterprise Server
- MWI, call transfer and conferencing originating from an Avaya Aura® Flare Communicator client
- Off-net call forwarding and mobility (extension to cellular)
- PRI trunking between Communication Server 1000 and Communication Manager
- Presence status with a one-X Mobile SIP client
- ACD agent as a Converged User
- PSTN calls routed thru the Communication Manager
- Avaya one-X Communicator for Communication Manager and Communication Server 1000
- Avaya 96xx phones
- Avaya Aura® Conferencing
- Avaya Aura® Messaging
- Communication Server 1000 features cannot be supported with Communication Manager, e.g. MADN (Multiple Appearance DN), Call Park, Call Pickup, Boss Secretary, etc

## 2.2. Test Results and Observations

Testing of the Collaboration Pack was completed successfully with the exception of the observations and limitations described below for Converged Users. These items are being addressed and updates will be provided as fixes are made available.

:

- Call transfers which are initiated from an Avaya SIP client (in the reference configuration this was the one-X Mobile client) to a Communication Server 1000 client result in no talk path
- Presence status for Avaya Flare Communicator on iPad as a Converged User does not get updated (from “busy” to “unknown”) upon termination of the call from a Communication Server 1000 client (the presence is updated if a call is attempted or answered from the client)
- Incorrect Calling Party Name and Number on transferred and conference calls: there are a number of different scenarios involving transferred and conference calls where the call display is not properly updated to reflect the true connected party on calls that are either transferred or involved in a conference call. E.g. after the call transfer was completed the tandemed call thru the Communication Server 1000 showed the party that initiated the transfer instead of the actual connected party

### 3. Reference Configuration

The reference configuration described throughout the Application Note is shown in **Figure 1**.



**Figure 1: Reference Configuration**

#### 3.1 Avaya Aura® Midsize Enterprise Solution Components

Avaya Aura® Solution for Midsize Enterprise Release 6.2 Template delivers the following applications as virtual machines running on System Platform 6.2:

- Communication Manager 6.2
- Communication Manager Messaging 6.2
- Session Manager 6.2
- System Manager 6.2
- Presence Services 6.1
- Utility Services 6.2
- Application Enablement Services 6.1.2


This Application Note will not cover the software installation of System Platform and the loading of the Midsize Enterprise Template. For more information and step by step instructions on the software installation of System Platform, the Midsize Enterprise Template and initial

configuration for Session Manager, Communication Manager and Presence Server see **Reference [1] thru [3] in Section 12.**

The screenshot shows the list of the applications installed and running on the server, as seen from the Virtual Machine Management screen in System Platform.



**Virtual Machine Management**  
 Virtual Machine List  
 System Domain Uptime: 5 days, 16 hours, 21 minutes, 38 seconds  
 Current template installed: Midsize\_Ent 6.2.0.0.3105 (smgr 6.2.12.0, aes 6.1.2.0.32, cm 06.2-02.0.823.0, utility\_server 6.2.0.0.15, sm 6.2.0.0.620120 06.01.00.00-0502) [Refresh](#)

	Name	Version	IP Address	Max Memory	Virtual CPUs	CPU Time	State	Application State
✓	<a href="#">Domain-0</a>	<a href="#">6.2.0.2.27</a>	135.9.146.128	864.0 MB	12	20h 22m 20s	Running	N/A
✓	<a href="#">sm</a>	<a href="#">6.2.0.0.620120</a>	135.9.146.132	5.0 GB	6	12h 11m 35s	Running	Running
✓	 <a href="#">cm</a>	<a href="#">06.2-02.0.823.0</a>	135.9.146.130	4.5 GB	1	5h 23m 49s	Running	Running
✓	 <a href="#">aes</a>	<a href="#">6.1.2.0.32</a>	135.9.146.136	2.0 GB	4	5h 13m 25s	Running	Running
✓	<a href="#">cdom</a>	<a href="#">6.2.0.2.27</a>	135.9.146.129	512.0 MB	1	3h 52m 55s	Running	N/A
✓	 <a href="#">utility_server</a>	<a href="#">6.2.0.0.15</a>	135.9.146.131	512.0 MB	1	45m 19s	Running	Running
✓	 <a href="#">presence_va</a>	<a href="#">06.01.00.00-0502</a>	135.9.146.134	12.0 GB	6	1h 54m 1s	Running	N/A
✓	 <a href="#">smar</a>	<a href="#">6.2.12.0</a>	135.9.146.135	6.0 GB	4	15h 27m 4s	Running	Running

Note that Application Enablement and Communication Manager Messaging are installed as part of the Midsize Enterprise Template, but since this application is not being used during this testing, the configuration of this service is not covered in this Application Note.

The other Avaya components used during this testing are:

- Avaya G430 Media Gateway
- Avaya Flare Communicator on iPad
- Avaya one-X® Communicator Mobile SIP for iOS on iPhone and iPod
- Avaya CallPilot 202i
- Avaya Communication Server 1000 IP and digital telephones

SIP trunks will be created between the Session Manager on the Collaboration Pack and Communication Server 1000 to carry outbound and inbound traffic for the collaboration clients. Calls destined to the PSTN from collaboration clients will be routed to the Communication Server 1000 via Session Manager.

Outbound calls to the PSTN originating from the collaboration clients will be first processed by Collaboration Pack for outbound feature treatment such as automatic route selection and class of service restrictions.



Note: The Avaya G430 Media Gateway configuration will not be covered in this App Note. Please refer to **Reference [4] in Section 12** for details.

### 3. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya Communication Server 1000E running on CPPM server	Release 7.5, Q+ Service_Pack_Linux_7.50_17_20120314.ntl
Avaya Aura <sup>®</sup> Midsize Enterprise (Session Manager, System Manager and Presence)	6.2 Template 3105
Avaya G430	FW 31.22.0
CallPilot (202i)	5.0 SU11
M3904/5	FW AA94
11xx & 12 xx UNISlim phones	FW 0625C8L
Avaya Flare Communicator on iPad	1.01
Avaya one-X Mobile SIP for iOS	1.04

**Table 1: Equipment/Software List**

## 4. Configure Avaya Communication Server 1000E

This section describes the details for configuring Avaya Communication Server 1000E to route calls to the Collaboration Pack as well as provide simultaneous ringing to Avaya Aura® SIP endpoints via Session Manager over a SIP trunk. It also includes details for configuring Presence Services for the Communication Server 1000E. This section does not include information on migrating the Network Routing Service (NRS) to Session Manager. Please see **Reference [5] in Section 12** for these migration steps.

These instructions assume the Communication Server 1000 has been registered a member of the System Manager Security framework. For more information on how to configure System Manager to integrate with the Avaya Unified Communications Management application, see **Reference [7] in Section 12**. **Note: If the UCM Primary Security Server is currently co-resident (with CS 1000 applications) that server will be required to be rebuilt as a member server.**

In addition, these instructions also assume the configuration of the CS 1000 Call Server and Signaling Server applications has been completed is configured to support UNISTim (IP) telephones, and Digital telephones. For information on how to administer these functions of Avaya Communication Server 1000E, see **References [6], [7], [8] and [9] in Section 12**.

Using the Avaya Unified Communications Management Element Manager interface, the following administration steps will be described:

- Enable Avaya Unified Communications Management Services in System Manager
- Launch Avaya Unified Communications Management web interface from System Manager
- Confirm Node and IP addresses
- Confirm Virtual Trunks and D-Channel
- Configure SIP Trunk to Session Manager
- Configure ESN – DSC or Special # route prefix for converging
- Configure Presence Service # and Presence Publisher
- Configure Presence Services for all Communication Server 1000 Users
- Save Configuration changes

**Note:** Some administration screens have been abbreviated for clarity.

Access the web based GUI of Avaya Aura® System Manager by using the URL “**http://<ip-address>/SMGR**”, where **<ip-address>** is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

### 4.1. Enable UCM Services in SMGR

For the UCM Services link to show up in the Home Console of SMGR first enable Common Console and select UCM Configured to “true”.

1. **Home /Services / Configurations / Settings / SMGR / Common Console**
2. UCM configured = "true"



## Avaya Aura® System Manager 6.2

Home /Services / Configurations / Settings / SMGR / Common Console

**Edit Profile: Common Console**

Common Console

\* Max No of tabs that can opened on the landing page : 5

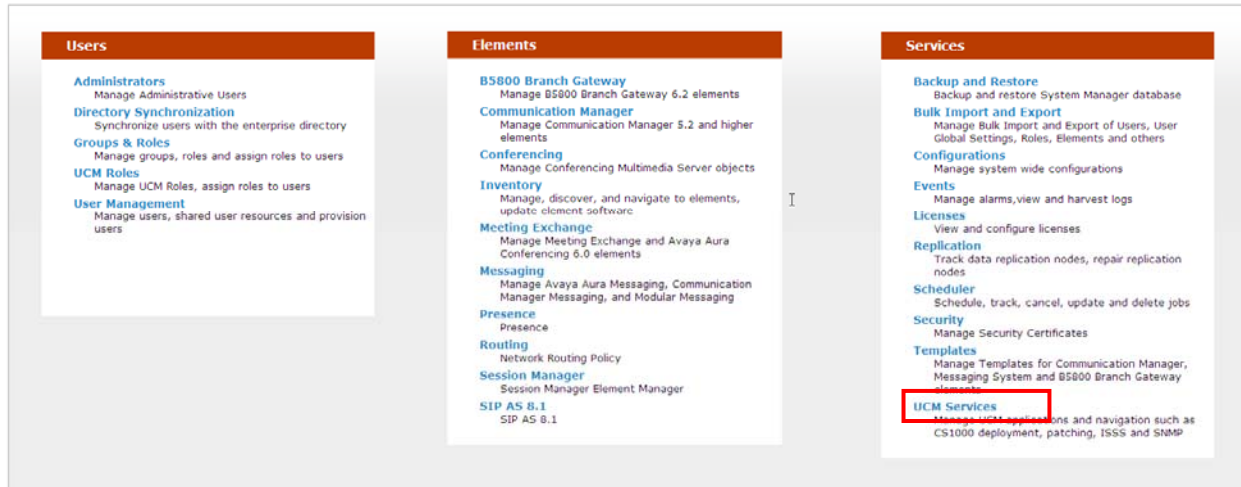
\* No Of Rows : 15

\* Max No of Records Selectable (Table) : 100

\* UCM Configured : true

\* Required

For the change to take into effect, logout of System Manager and log back-in. Avaya Aura® System Manager Home Page will be displayed. Use the **Services** category on the right side and select **UCM Services** for CS1000 management.



The Avaya Unified Communications Management **Elements** page will open in a new browser window. Select the EM **Element Name** corresponding to “CS1000” in the **Element Type** column.

Host Name: 10.80.111.105 Software Version: 02.20\_SMGR-SNAPSHOT(3925) User Name admin

### Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

	Element Name	Element Type	Release	Address	Description
1	<a href="#">smgr61-smgr.avaya.com (primary)</a>	Base OS	7.5	10.80.111.105	Base OS element
2	<a href="#">EM on cs1000r75</a>	CS1000	7.5	10.80.51.60	New element
3	<a href="#">cs1000r75.avaya.com (member)</a>	Linux Base	7.5	10.80.50.60	Base OS element
4	10.80.51.62	Media Gateway Controller	7.5	10.80.51.62	New element

## 4.2. Confirm Node and IP Addresses

Expand **System** → **IP Network** on the left panel and select **Nodes: Servers, Media Cards**.

The **IP Telephony Nodes** page is displayed as shown below. Click “<Node id>” in the **Node ID** column to view details of the node. In the sample configuration, “1006” was used.

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - IP Network
    - **Nodes: Servers, Media Cards**
    - Maintenance and Reports
    - Media Gateways
    - Zones
    - Host and Route Tables
    - Network Address Translation (NAT)

Managing: 135.9.139.206 Username: admin  
System » IP Network » IP Telephony Nodes

### IP Telephony Nodes

Click the Node ID to view or edit its properties.

Add... Import... Export... Delete				
<input type="checkbox"/> Node ID ^	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4
<input type="checkbox"/> 1006	1	SIP Line, LTPS, PD, Presence Publisher, Gateway - (SIPGw)		135.9.146.54
Show: <input checked="" type="checkbox"/> Nodes <input type="checkbox"/> Component servers and cards <input checked="" type="checkbox"/> IPv6 address				

The **Node Details** screen is displayed with additional details as shown below. Make a note of the **Node IP address**, **Call server IP address** and **Signaling Server TLAN IPv4** address fields highlighted below as these values are used to configure other sections.

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - IP Network
    - **Nodes: Servers, Media Cards**
    - Maintenance and Reports
    - Media Gateways
    - Zones
    - Host and Route Tables
    - Network Address Translation (NAT)
    - QoS Thresholds
    - Personal Directories
    - Unicode Name Directory
  - + Interfaces
    - Engineered Values
    - Emergency Services
    - Geographic Redundancy
    - Software
- Customers
  - Routes and Trunks
    - Routes and Trunks
    - D-Channels
    - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views

Managing: 135.9.139.206 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details

### Node Details (ID: 1006 - SIP Line, LTPS, PD, Presence Publisher, Gateway (SIPGw))

Node ID: 1006 * (0-9999)	TLAN address type: <input checked="" type="radio"/> IPv4 only <input type="radio"/> IPv4 and IPv6
Call server IP address: 135.9.139.206 *	
<b>Embedded LAN (ELAN)</b> Gateway IP address: 135.9.139.254 * Subnet mask: 255.255.254.0 *	
<b>Telephony LAN (TLAN)</b> Node IPv4 address: 135.9.146.54 * Subnet mask: 255.255.255.0 * Node IPv6 address:	
* Required Value.	
Save Cancel	

### Associated Signaling Servers & Cards

Select to add		Add	Remove	Make Leader	Print   Refresh	
<input type="checkbox"/>	Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/>	cs1knc-cppm	Signaling_Server	LTPS, Gateway, PD, Presence Publisher, IP Media Services	135.9.139.205	135.9.146.53	Leader
Show: <input type="checkbox"/> IPv6 address						
Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.						

### 4.3. Confirm Virtual D-Channel, Routes and Trunks

Avaya Communication Server 1000E Call Server utilizes a virtual D-channel and associated Route and Trunks to communicate with the Signaling Server and Session Manager. This section describes the steps to verify that this administration has already been completed.

#### 4.3.1. Confirm Virtual D-Channel Configuration

Expand **Routes and Trunks** on the left navigation panel and select **D-Channels**. The screen below shows all the D-channels administered on the sample configuration.

**AVAYA** **CS1000 Element Manager**

Managing: 135.9.139.206 Username: admin  
Routes and Trunks » D-Channels

### D-Channels

#### Maintenance

- [D-Channel Diagnostics](#) (LD 96)
- [Network and Peripheral Equipment](#) (LD 32, Virtual D-Channels)
- [MSDL Diagnostics](#) (LD 96)
- [TMDI Diagnostics](#) (LD 96)
- [D-Channel Expansion Diagnostics](#) (LD 48)

#### Configuration

Choose a D-Channel Number:  and type:

- Channel: 3	Type: DCH	Card Type: TMDI	Description: PDRtoBeta	<input type="button" value="Edit"/>
- Channel: 15	Type: DCH	Card Type: DCIP	Description: SIPLine	<input type="button" value="Edit"/>

In the sample configuration, there is a single D-channel assigned to “**Channel: 15**” with “**Card Type: DCIP**”. Specifying “**DCIP**” as the type of channel indicates the D-channel is a virtual D-channel.

#### 4.3.2. Confirm Routes and Trunks Configuration

In addition to configuring a virtual D-channel, a **Route** and its associated **Trunks** need to be administered.

Ensure this route and trunk member’s route to the Session Manager Asset IP address for SIP traffic.

Expand **Routes and Trunks** on the left navigation panel and select **Routes and Trunks** (not shown) to verify a route with enough trunks to handle the expected number of simultaneous calls has been configured.

As shown in the screen below, “**Route 100**” has been configured with 32 trunks which indicate the system can handle 32 simultaneous calls out to Session Manager over SIP.

Managing: [135.9.139.206](#) Username: admin  
Routes and Trunks » Routes and Trunks

## Routes and Trunks

- Customer: 0	Total routes: 3	Total trunks: 87	Add route	
+ Route: 3	Type: DID	Description: SIPTOBETA	Edit	Add trunk
+ <a href="#">Route: 10</a>	Type: TIE	Description: SIPLINE	Edit	Add trunk
- <b>Route: 100</b>	<b>Type: TIE</b>	Description: <b>SIPTOME</b>	Edit	Add trunk
+ Trunk: 1 - 32	Total trunks: 32			

Select **Edit** to verify the configuration.

The details of the virtual Route defined for sample configuration is shown below. Verify “**SIP (SIP)**” has been selected for **Protocol ID for the route (PCID)** field and the **Node ID of signaling server of this route (NODE)** and **D channel number (DCH)** fields match the values identified in the previous section.

## Customer 0, Route 100 Property Configuration

### - Basic Configuration

Route data block (RDB) (TYPE) :	RDB
Customer number (CUST) :	00
Route number (ROUT) :	100
Designator field for trunk (DES) :	SIP TO ME
Trunk type (TKTP) :	TIE
Incoming and outgoing trunk (ICOG) :	Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD) :	79100
Trunk type M911P (M911P) :	<input type="checkbox"/>
The route is for a virtual trunk route (VTRK) :	<input checked="" type="checkbox"/>
- Zone for codec selection and bandwidth management (ZONE) :	00010 (0 - 8000)
- Node ID of signaling server of this route (NODE) :	1006 (0 - 9999)
- Protocol ID for the route (PCID) :	SIP (SIP)
- Print correlation ID in CDR for the route (CRID) :	<input type="checkbox"/>
Integrated services digital network option (ISDN) :	<input checked="" type="checkbox"/>
- Mode of operation (MODE) :	Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH) :	15 (0 - 254)
- Interface type for route (IFC) :	Meridian M1 (SL1)
- Private network identifier (PNI) :	00000 (0 - 32700)
- Network calling name allowed (NCNA) :	<input checked="" type="checkbox"/>
- Network call redirection (NCRD) :	<input type="checkbox"/>
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) :	<input type="checkbox"/>
- Channel type (CHTY) :	B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP) :	Unknown Call type (UKWN)
- Insert ESN access code (INAC) :	<input type="checkbox"/>
- Integrated service access route (ISAR) :	<input type="checkbox"/>
- Display of access prefix on CLID (DAPC) :	<input type="checkbox"/>
- Mobile extension route (MBXR) :	<input type="checkbox"/>
- Mobile extension outgoing type (MBXOT) :	National number (NPA)

## 4.4. Configure SIP Trunk to Avaya Aura® Session Manager

Expand System - IP Network - Nodes: Servers, Media Cards.

Select “1006” in the **Node ID** column (not shown) to edit configuration settings of node.

Using the scroll bar on the right side of the screen, navigate to the **Applications** section on the screen and select the **Gateway (SIPGw)** link (not shown).



On the **Node ID: 1006 - Virtual Trunk Gateway Configuration Details** page, confirm the following values and use default values for remaining fields.

- **SIP domain name:** Enter name of domain.  
In the sample configuration, “**us.global.avaya.com**” was used.
- **Local SIP port:** Enter “**5060**”
- **Gateway endpoint name:** Enter descriptive name
- **Application node ID:** Enter “<Node id>”.  
In the sample configuration, “**1006**” was used.

The values defined for the sample configuration are shown below.

### Node ID: 1006 - Virtual Trunk Gateway Configuration Details

The screenshot shows the configuration page for Node ID 1006. The 'General' tab is selected. The 'Vtrk gateway application' is set to 'SIP Gateway (SIPGw)'. The 'SIP domain name' is 'us.global.avaya.com', 'Local SIP port' is '5060', 'Gateway endpoint name' is 'node1006', and 'Application node ID' is '1006'. The 'Virtual Trunk Network Health Monitor' section is also visible, with a checkbox for 'Monitor IP addresses (listed below)' and a list of 'Monitor IP' addresses.

Scroll down to **SIP Gateway Settings - Proxy or Redirect Server:** section of the page.

Under **Proxy Server Route 1:** section, enter the following values and use default values for remaining fields.

- **Primary TLAN IP address:** Enter IP address of the Session Manager SIP signaling asset “**135.9.146.133**”
- **Port:** Enter “**5060**”
- **Transport protocol:** Select “**TCP**”

**Note:** TCP was used for the sample configuration. However, TLS would typically be used in production environments. For more information on configuring the system to use TLS, see **Reference [5]** in **Section 12**.

The values defined for the sample configuration are shown below.

## Node ID: 1006 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Port: 5060 (1 - 65535)

Transport protocol: TCP

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 135.9.146.133  
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: ☐ Support registration  
☐ Primary CDS proxy

Secondary TLAN IP address: 0.0.0.0  
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN

Click **Save** on the **Node Details** screen (not shown).

Select **Transfer Now** on the **Node Saved** page as shown below.

Managing: 135.9.139.206 Username: admin  
System » IP Network » IP Telephony Nodes » Node Saved

### Node Saved

Node ID: 1006 has been saved on the call server.

The new configuration must also be transferred to associated servers and media cards.

**Transfer Now...** You will be given an option to select individual servers, or transfer to all.

**Show Nodes** You may initiate a transfer manually at a later time.

Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed.

**Synchronize Configuration Files (Node ID <1006>)**

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart\* of applications on affected server(s) when complete.

[Print](#) | [Refresh](#)

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cs1knse-cppm	Signaling_Server	LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

\* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

Enter ☒ associated with the appropriate Call Server and click **Start Sync**. The screen will automatically refresh until the synchronization is finished. The **Synchronization Status** field will update from **Sync required** (as shown) to **Synchronized** (not shown).

After synchronization completes, click **Restart Applications** to use new SIP Gateway settings.

## 4.5. Configure ESN for Route List Index and Digit Manipulation

This section provides the configuration of the routing used in the sample configuration for routing calls over a SIP Trunk between the Communication Server 1000 on the one side and Session Manager on the Collaboration Pack.

**Note:** The CS1000 Dialing plan and Collaboration Pack routing with adaptations will normalize the dial plan allowing Convergence of User endpoints. The routing rules defined in this section are an example and were used in the reference configuration. Other routing policies may be appropriate for different customer networks.

### Step 1: Create Route List Index

Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**.

Select **Route List Block (RLB)**

The **Route List Blocks** screen is displayed. Enter an available route list index number in the **Please enter a route list index** field and click **to Add** as shown below.

Managing: [135.9.139.206](#) Username: admin  
Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) » Customer 00 » Network Control & Services » Route List Blocks

---

## Route List Blocks

Please enter a route list index  ( 0 - 1999 )

---

Under the **Options** section, select “<**Route id**>” of the route identified in **Section 4.3.2** in the **Route Number** field and use default values for remaining fields as shown below.

---

## Route List Block

### General Properties

Number of Alternate Routing Attempts:  ( 1 - 10 )  
Initial Set:  ( 0 - 64 )  
Set Minimum Facility Restriction Level :   
Overlap Length:  ( 0 - 24 )  
Extended Local Calls: ☐  
Route List Index:   
Entry Number for the Route List:  ( 0 - 63 )

### Indexes

Time of Day Schedule:  ▼  
Facility Restriction Level:  ( 0 - 7 )  
Digit Manipulation Index:  ▼  
ISL D-Channel Down Digit Manipulation Index:  ( 0 - 1999 )  
Free Calling Area Screening Index:  ▼  
Free Special Number Screening Index:  ▼  
Business Network Extension Route: ☐  
Incoming CLID Table:  ( 0 - 1 )

### Options

Local Termination entry: ☐  

Route Number:  ▼

  
Skip Conventional Signaling: ☐  
Display Originator's Information: ☐  
Use Tone Detector: ☐  
Conversion to LDN: ☐  
Expensive Route: ☐  
Strategy on Congestion:  ▼  
- QSIG Alternate Routing Causes:  ▼  
Preferred Routing:  ▼  
ISDN Drop Back Busy:  ▼

Click **Save** (not shown) to save new Route List Block definition.

## Step 2: Create Distant Steering Code

This Digit string will be used as the new unique “Converged Route Prefix” in each CS1000 Users PCA to route calls to the Collaboration Pack via the Session Manager.

Expand **Dialing and Numbering Plans** on the left and select **Electronic Switched Network**. Select **Distant Steering Code (DSC)** under the **Coordinated Dialing Plan (CDP)** section on the **Electronic Switched Network (ESN)** page as shown below.

Select “**Add**” from the drop-down menu and enter the dialed prefix for external calls to be routed over SIP trunk to Session Manager in the **Please enter a distant steering code** field. For the sample configuration, “**23**” was used since SIP endpoints registered to Session Manager were assigned extensions starting with “**23**”. Click to **Add** as shown below.

---

Managing: [135.9.139.206](#) Username: admin  
Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) » Customer 00 » Coordinated Dialing Plan (CDP) » Distant Steering Code List

---

### Distant Steering Code List

▼

Please enter a distant steering code

---

Select the **Flexible Length of number of digits** to be “**7**”. This DSC is routed to the Route (RLI) **100** built in the step above.

Enter the following values and use default values for remaining fields.

- **Flexible Length number of digits:** Enter number of digits in dialed numbers  
In the sample configuration, “**7**” was used.
- **Route List to be accessed for trunk steering code:** Select “<id>” of Route List Index to be “**100**”.

Click **Submit** to save new Distant Steering Code definition.

## Distant Steering Code

Distant Steering Code:

Flexible Length number of digits:  ( 0 - 10 )

Display:

Remote Radio Paging Access: ☐

Route List to be accessed for trunk steering code:

Collect Call Blocking: ☐

Maximum 7 digit NPA code allowed:

Maximum 7 digit NXX code allowed:

## 4.6. Configure Avaya Communication Server 1000 Presence Services

To configure Presence Services with Communication Server 1000 follow **Reference [10], [11] and [12]** in **Section 12**. Please consider the following additional configuration information.

Note : System Manager SP2 is required for this procedure.

### 4.6.1. TLS & Certificates section

Replacing the Session Manager default certificate:

In the document referenced above in the specific section titled “TLS configuration between CS 1000 and Session Manager”, the Common Name is defined as the “Fully Qualified Domain Name” of the Session Manager.

Need to replace the Session Manager default certificate as it uses a hard coded Common Name.

1. In System Manager, navigate to **Elements > Inventory**.
2. In the navigation tree, click **Manage Elements**.
3. In the Entities section, select a Session Manager instance.
4. From the **More Actions** menu, click **Configure Identity Certificates**.
5. Click **security module**, and click the **Replace**.
6. Click **Replace this Certificate with Internal CA Signed Certificate**.
7. Complete the fields for **Common Name**, **Organization Unit**, **Organization**, **Country**, and click **Key Algorithm** and **Key Size**.
8. Verify your data, and click **Commit**.

**Common Name** is defined as Fully Qualified Domain Name (FQDN) of your Session Manager asset.  
e.g. C=US, O=Avaya, CN=gmi-alphame-asset.global2.avaya.com

To change the Certificate Common Name Identify navigate from the Home page to:

**Inventory - Manage Elements - Select Session Manager - More Actions - Configure Identity Certificate**

## Manage Elements

### Elements

More Actions ▾

18 Items | Refresh | Show 15 ▾

<input type="checkbox"/>	Name	Node	Type
<input type="checkbox"/>	135.9.139.206	135.9.139.206	UCMApp
<input type="checkbox"/>	135.9.139.207	135.9.139.207	UCMApp
<input type="checkbox"/>	Corporate Directory	135.9.146.135	UCMApp
<input type="checkbox"/>	cs1knse-cppm.global2.avaya.com (member)	135.9.146.53	UCMApp
<input type="checkbox"/>	EM on cs1knse-cppm	135.9.139.206	UCMApp
<input type="checkbox"/>	gmi-alphame-aes	135.9.146.136	Application Enablement Services
<input type="checkbox"/>	gmi-alphame-cm	135.9.146.130	Communication Manager
<input type="checkbox"/>	gmi-alphame-cm-Messaging	135.9.146.130	Messaging
<input type="checkbox"/>	gmi-alphame-pres	135.9.146.134	Presence Services
<input checked="" type="checkbox"/>	gmi-alphame-sm	135.9.146.132	Session Manager

**Inventory - Manage Elements - Select Session Manager – More Actions - Configure Identity Certificate - Select Security Module**



## Identity Certificates

### Identity Certificates

[Replace](#)[Export](#)[Renew](#)3 Items | [Refresh](#)

	Service Name	Common Name	Valid To
<input type="radio"/>		smmgmt	Sat Mar 08 15:56:27 MST 2014
<input checked="" type="radio"/>		securitymodule	Wed Apr 09 12:58:13 MDT 2014
<input type="radio"/>		spiritalias	Sat Mar 08 15:56:40 MST 2014

Select : None

### Certificate Details

**Subject Details** **Valid From** **Key Size** **Issuer Name** **Finger Print** 

Note as seen in the screen shot above the Certificate Details the Common Name.

### 4.6.2. Change Session Manager Access Point Address:

This change is required for the trust management between Session Manager and Communication Server 1000. The Midsize Enterprise template is inserting by default the local host but this must be changed to the Session Manager IP address. To make this change navigate from System Manager Home to:

Inventory → Manage Elements → Select your Session Manager → Edit → Access Point.


## Manage Elements

### Elements

18 Items | Refresh | Show 15

<input type="checkbox"/>	Name	Node	Type	Version
<input type="checkbox"/>	135.9.139.206	135.9.139.206	UCMApp	
<input type="checkbox"/>	135.9.139.207	135.9.139.207	UCMApp	
<input type="checkbox"/>	Corporate Directory	135.9.146.135	UCMApp	
<input type="checkbox"/>	cs1knse-cppm.global2.avaya.com (member)	135.9.146.53	UCMApp	
<input type="checkbox"/>	EM on cs1knse-cppm	135.9.139.206	UCMApp	
<input type="checkbox"/>	gmi-alphame-aes	135.9.146.136	Application Enablement Services	
<input type="checkbox"/>	gmi-alphame-cm	135.9.146.130	Communication Manager	
<input type="checkbox"/>	gmi-alphame-cm-Messaging	135.9.146.130	Messaging	
<input type="checkbox"/>	gmi-alphame-pres	135.9.146.134	Presence Services	
<input checked="" type="checkbox"/>	gmi-alphame-sm	135.9.146.132	Session Manager	
<input type="checkbox"/>	gmi-alphame-smgr.global2.avaya.com (primary)	135.9.146.135	UCMApp	
<input type="checkbox"/>	IPSec	135.9.146.135	UCMApp	
<input type="checkbox"/>	Numbering Groups	135.9.146.135	UCMApp	
<input type="checkbox"/>	Patches	135.9.146.135	UCMApp	
<input type="checkbox"/>	Secure FTP Token	135.9.146.135	UCMApp	

Edit the **Host** from “localhost” to the Session Manager IP address. For the reference configuration this is “135.9.146.132”. Select **Save** then **Commit**.

	Name	Access Point Type	Protocol	Host	Port
	Session Manager	TrustManagement	jnp	135.9.146.132	1299
Select : None					

Access Point Details

\* Name

Session Manager

Access Point Type

TrustManagement

\* Container Type

JBOSS

\* Protocol

jnp

\* Host

135.9.146.132

\* Port

1299

Path

None

\* Order

0

Description

Save

Cancel

#### 4.6.3. Verify Communication Server 1000 UCM Security Certificates:

For Communication Server 1000 clients to push presence updates to Presence Services they need to communicate over SIP TLS.

Need to confirm the **CS1000 Endpoint Details – Certificate** Service Profile – SIP TLS is signed. See the screen shot below.

Navigate to **UCM Services - Security – Certificates**

Select **Linux Base** as element type to view **Endpoint Details**. See screen shot below.

- Network
  - Elements
- CS 1000 Services
  - Corporate Directory
  - IPSec
  - Numbering Groups
  - Patches
  - SNMP Profiles
  - Secure FTP Token
  - Software Deployment
- User Services
  - Administrative Users
  - External Authentication
  - Password
- Security
  - Roles
  - Policies
  - Certificates
  - Active Sessions

Host Name: gmi-alphame-smgr.global2.avaya.com    Software Version: 02.20\_SMGR-SNAPSHOT(5167)    User Name admin

### Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Certificate Endpoints

Private Certificate Authority

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When multiple logical elements reside on a single base server, only the base endpoint is shown.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
1	135.9.146.53	Linux Base	cs1kncse-cppm.global2.avaya.com (memb...	4
2	135.9.146.135	Base OS	gmi-alphame-smgr.global2.avaya.com (pr...	4

#### Endpoint Details

Details for the selected endpoint.

##### Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	cs1kncse-cppm.global2.avaya.com	Mar 24, 2022
2	DTLS	none		
3	Web SSL	none		
4	SIP TLS	signed	GMI-CS1K	Apr 7, 2022

##### Certificate Authorities

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1	default	Mar 6, 2022	yes	/CN=default/OU=MGMT/O=AV...	
2	gmi-alphame-smgr....	Feb 1, 2035	yes	/O=AVAYA/ST=ON/L=BVV/C=...	Apr 9, 2012

#### 4.6.4. Communication Server 1000 Presence User Agent Configuration:

To enable Presence Services on the Communication Server 1000 the following is required to be configured. For detailed steps please refer to **Reference [13]** in **Section 12**.

The following Communication Server 1000 attributes are required to be configured:

- **ELAN AML**
- **VAS ID**
- **ACD DN**
- **CDN**

The **ELAN AML Link** can be configured via LD17 or via System Manager.

Navigate to **UCM Services – Interfaces – Application Module Link**. For the reference configuration, port number “**32**” and Description “**Presence**”.

**AVAYA** **CS1000 Element Manager**

Managing: 135.9.139.206 Username: admin  
System » Interfaces » Application Module Link » New Application Module Link

**New Application Module Link**

Port number:  (16 - 127)  
AML over ELAN

Description:

☐ Link control system parameters

Maximum octets:  (per HDLC frame)

\* Required value.

To configure **VAS ID for AML** please follow the following steps in LD17.

Command/Prompt	Command/User Response(s)	Description
REQ	CHG	Change ADAN
TYPE	VAS	
VAS	New	New a VAS
VSID	vasID	The VAS ID number – <b>e.g. “32”</b> was used for the reference configuration.
ELAN	ELAN#	ELAN number, should match the one configured in previous step, <b>e.g. “32”</b> was used for the reference configuration.

To configure **ACD DN** please follow the following steps in LD23.

Command/Prompt	Command/User Response(s)	Description
REQ	New	New ACD
TYPE	ACD	Customer number  An ACD DN to be used when configuring the CDN (PSDN) for Presence. <b>e.g. “5000”</b> was used for the reference configuration.
CUST	custNum	
ACDN	Xxxx	

To configure **CDN** please follow the following steps in LD23.

Command/Prompt	Command/User Response(s)	Description
REQ	New	New CDN
TYPE	CDN	Customer number. <b>e.g. “0”</b> was used for the reference configuration.  A number to be used by the Presence Publisher. This CDN is used within the ACD 5000 as the PSDN for each CS1000 user. <b>e.g. “3000”</b> was used for the reference configuration. This # must be fit into your Communication Server 1000 overall dialplan.
CUST	custNum	
CDN	Xxxx	

CDSQ	Yes	This needs to be “yes”, so the presence activity is sent to PP.
DFDN	Xxxx	ACD DN <b>5000</b> configured in the table as above.

#### 4.6.5. Configure Presence Publisher to Session Manager

The following configuration is to enable the publishing of Presence updates for Communication Server 1000 endpoints.

Navigate to **UCM Services – EM – IP Network – Nodes: servers, Media Cards-Node 1006**  
Using the scroll bar on the right side of the screen, navigate to the **Applications** section on the screen and select the **Presence Publisher** link.

Managing: 135.9.139.206 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details

**Node Details (ID: 1006 - SIP Line, LTPS, PD, Presence Publisher, Gateway ( SIPGw ))**

Gateway IP address: 135.9.139.254 \* Node IPv4 address: 135.9.146.54 \*  
Subnet mask: 255.255.254.0 \* Subnet mask: 255.255.255.0 \*  
Node IPv6 address:

**IP Telephony Node Properties**

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

**Applications (click to edit configuration)**

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher**
- IP Media Services

Enter in the following for the fields below shown in the screen shot. Note these are used for the reference configuration.

- Presence Publisher: **Enable**
- Type : **Aura PS**
- IM and Presence server FQDN: Enter the **domain** of the presence service. (not the FQDN of the Presence server. “**pres.ips.avaya.com**”)
- Presence Server IP: **IP address** of the Presence Service, “**135.9.146.134**”
- Port: **15061**
- SIP Transport: **TLS** ( TLS must be used for Presence )
- Presence Publisher SIP Port: **5080** (sip port must be unique to the CS1000 over the virtual trunk)
- Presence Publisher TLS Port: **5061**
- Security Policy: **Best Effort**

## Node ID: 1006 - Presence Publisher Configuration Details

Presence Publisher: ☒ Enable presence publisher service

IM and Presence server type:

**Presence Application Settings**

IM and presence server FQDN:  \*

**Presence Server**

IM and Presence server IP:  \*

The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port:  \* (1 - 65535)

SIP transport:

Presence publisher SIP port:  \* (1 - 65535)

Presence publisher TLS port:  \* (1 - 65535)

Security policy:

Number of byte re-negotiation:

Enter in the following for the fields below shown in the screen shot. Note these are used for the reference configuration.

- Outbound Proxy: **Session Manager asset sip service IP address, "135.9.146.133"**
- Port: **5061**
- Transport: **TLS**
- Secondary: **5061, TLS** can be used as secondary transport to Session Manager
- Call Server Settings:
  - Customer: **0** - Select the CS 1000 customer #
  - PSDN : **Service # (DN) the CDN built** of the publisher user agent built in above section which is **"3000"**.



☐ x509 Certificate authentication enabled

**Outbound Proxy Server**

Primary outbound proxy IP:  \*

The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port:  \* (1 - 65535)

SIP transport:

Secondary outbound proxy IP:  \*

The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port:  \* (1 - 65535)

SIP transport:

**Call Server Settings**

Customer number:

Presence service DN (PSDN):  \*

Click **Save** on the **Node Details** screen (not shown).

Select **Transfer Now** on the **Node Saved** page as shown below.

Managing: 135.9.139.206 Username: admin  
System » IP Network » IP Telephony Nodes » Node Saved

---

**Node Saved**

Node ID: 1006 has been saved on the call server.

The new configuration must also be transferred to associated servers and media cards.

You will be given an option to select individual servers, or transfer to all.

You may initiate a transfer manually at a later time.

Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed.

**Synchronize Configuration Files (Node ID <1006>)**

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart\* of applications on affected server(s) when complete.

[Print](#) | [Refresh](#)

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cs1knse-cppm	Signaling_Server	LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

\* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

Enter ☒ associated with the appropriate Call Server and click **Start Sync**. The screen will automatically refresh until the synchronization is finished. The **Synchronization Status** field will update from **Sync required** (as shown) to **Synchronized** (not shown).

After synchronization completes, click **Restart Applications** to use new SIP Gateway settings.

#### 4.6.6. Configure Presence Services for all Communication Server 1000 Users

To enable Presence Services for each Communication Server 1000 user phone the following features must be configured as follows:

1. Presence Allowed (PREA) = “**Allowed**”
2. Services DN (PSDN) = “**3000**”

Navigate to **UCM Services - Elements – EM-Phones**. Select “Customer”, Value “0” then choose all the phone types that are to be configured. Select **More Actions “Edit”**.

## Search For Phones

Criteria:  Value:

Phones Found (29)

<input type="button" value="Add..."/> <input type="button" value="Import..."/> <input type="button" value="Retrieve..."/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/>					
<input checked="" type="checkbox"/>	Customer	TN		Designation	Phone Type*
1 <input checked="" type="checkbox"/>	0	096 0 00 06		GMI	1120
2 <input checked="" type="checkbox"/>	0	096 0 00 07		GMI	1120
3 <input checked="" type="checkbox"/>	0	096 0 00 21		1120	1120
4 <input checked="" type="checkbox"/>	0	096 0 00 29		1120	1120
5 <input checked="" type="checkbox"/>	0	096 0 00 00	52001	GMI	1140
6 <input checked="" type="checkbox"/>	0	096 0 00 11	52008	1140	1140
7 <input checked="" type="checkbox"/>	0	096 0 00 15	52101	GMI	1140
8 <input checked="" type="checkbox"/>	0	096 0 00 27	52801	1140	1140
9 <input checked="" type="checkbox"/>	0	096 0 00 13	52100	GMI	1185
10 <input checked="" type="checkbox"/>	0	096 0 00 03	52005	1220	1220

Add “**PREA-Presence**” and “**PSDN-Presence Services DN**” Fields.

Managing: [EM on cs1knse-cppm\(135.9.139.206\)](#)  
 Phones»Bulk Phone Edit

## Bulk Phone Edit (10 phones)

Field:

Select a Click on:

Note: F

- OLA-Outgoing Line Preference
- OPS-On/Off Premise Extension
- OUOA-Observe Using SCL
- OVDA-Override Another Busy Station
- PAR-Parity for NT Menu Dialing
- PBDO-Port Busy on DTR Off
- PCA\_TYPE-Generic or Microsoft OCS2007 PCA
- PCWA-Presence Call Waiting
- PGNA-PAGNET
- PHTA-Presence Hunting
- PKCH/OKCH-Charge Prime Key DN/Charge Originating Key DN
- PLEV-Override Priority Level
- PREA-Presence**
- PRPD-Port Priority Presentation Status
- PRI-ACD Agent Priority Level
- PRIMEDN-Prime DN
- PRM-Terminal User Prompts
- PRMA-DSN Station Loop Preemption
- PRPD-Priority Call Pick-up Status
- PSDN-Presence Service DN**
- PRPD-Port Priority Presentation Status

Select Old Value and New Value (as shown below) and select “**Update Phones**”.

### Bulk Phone Edit (1 phones)

Field: PSDN-Presence Service DN

	Field*	Old Value	New Value
1	<input checked="" type="checkbox"/> PREA-Presence	*	Allowed
2	<input checked="" type="checkbox"/> PSDN-Presence Service DN	*	3000

Confirm changes are successful (screen not shown).

## 4.7. Save Configuration

Expand **Tools** → **Backup and Restore** on the left navigation panel and select **Call Server**.

Select **Backup** (not shown) and click **Submit** to save configuration changes as shown below.

**AVAYA** **CS1000 Element Manager**

Managing: **10.80.51.60** Username: admin  
Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup

### Call Server Backup

Action

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - + Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - + IP Network
  - + Interfaces
    - Engineered Values
  - + Emergency Services
  - + Software
- Customers
- Routes and Trunks
  - Routes and Trunks
  - D-Channels
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views
  - Lists
  - Properties
  - Migration
- Tools
  - Backup and Restore
    - **Call Server**
    - Personal Directories

Backup process will take several minutes to complete. Scroll to the bottom of the page to verify the backup process completed successfully as shown below.

```
.  
Backing up reten.bkp to "/var/opt/nortel/cs/fs/cf2/backup/single"  
Database backup Complete!  
TEMU207
```

```
Backup process to local Removable Media Device ended successfully.
```

Configuration of Communication Server 1000 is complete.

## 5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager to receive and route calls over the SIP trunk between Communication Server 1000 and the Collab Pack.

These instructions assume other administration activities have already been completed, with the Avaya Midsize Enterprise Template installation, such as defining the SIP entity for Session Manager and defining the network connection between System Manager and Session Manager. For more information on these activities, see **References [1],[2] and [3] in Section 12.**

Upon completion of the Avaya Midsize Enterprise Template installation and configuration the following Session Manager configuration tasks are required to align with the Communication Server 1000.

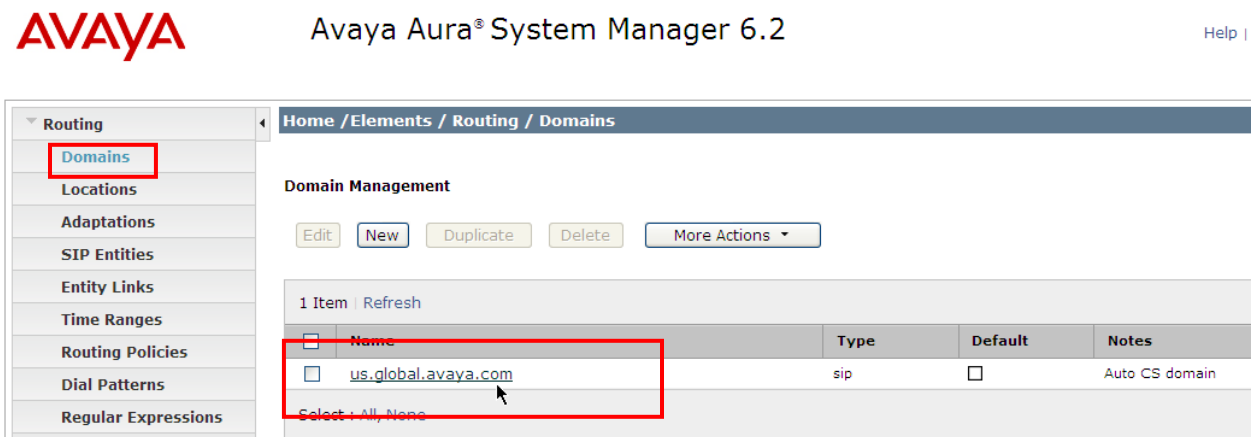
Specifically, the following administration activities will be described:

- Verify SIP Domains (with the Avaya Communication Server 1000 SIP domain)
- Define Location for Avaya Communication Server 1000
- Configure the Adaptation Module designed for Avaya Communication Server 1000 Release 7.5
- Define SIP Entities corresponding to Avaya Communication Server 1000 and Avaya Communication Manager
- Define Entity Links describing the SIP trunk and Presence link between Avaya Communication Server 1000E and Session Manager and the SIP trunk between Avaya Communication Manager and Session Manager
- Define an Entity Link describing the SIP trunk used for Presence services between the Communication Server 1000 and Session Manager.
- Define Routing Policies, which control call routing between the SIP Entities.
- Define Dial Patterns, which govern to which SIP Entity a call is routed.
- Define dial patterns for Communicator Server 1000 phones, MWI notification, PSTN access and PCA calls

**Note:** Some administration screens have been abbreviated for clarity.

## 5.1. Verify SIP Domains

Expand **Elements - Routing** and select **Domains** from the left navigation menu and verify that the Domain Name is the same as the Communication Server 1000 SIP Gateway Domain as shown in Section 4.4. In this sample configuration “**us.global.avaya.com**” was used. If the environment has pre-defined SIP domain it should be used here.



## 5.2. Define Location for Avaya Communication Server 1000

Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

Expand **Elements - Routing** and select **Locations** from the left navigational menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.  
“**Westminster, CO, USA**” was used for reference configuration.
- **Notes:** Add a brief description. [Optional]

Click **Commit** to save.

The screen below shows the Location defined for Communication Server 1000 in the sample configuration.



Routing

- Domains
- Locations**
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies

Home / Elements / Routing / Locations

Location Details

General

\* Name: Westminster, CO, USA

Notes: CS1000 Entity

### 5.3. Configure Adaptation Module

To enable calls between stations on Communication Server 1000 and SIP endpoints registered to Session Manager, Session Manager should be configured to use an Adaptation Module designed for Communication Server 1000 to convert SIP headers in messages sent by Communication Server 1000 to the format used by other Avaya products and endpoints. All calls to the Communication Server 1000 will have the Communication Server 1000 NARS access code ('1' is used for this reference configuration) added as they leave Communication Manager. The Session Manager will route all digit strings with a leading '1' to the Communication Server 1000. It will be necessary to delete the leading '1' for those calls that terminate within the Communication Server 1000 (station calls and Call Pilot).

Expand **Elements - Routing** and select **Adaptations** from the left navigational menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.



- **Adaptation Name:** Enter an identifier for the Adaptation Module **Module Name:** Select “CS1000Adapter” from drop-down menu
- **Module Parameter: “fromto=true”** this will ensure that the ‘from’ header is updated  
In the **Digit Conversion for Outgoing from SM** section, click **Add** and enter the following values.

Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address To Modify	Notes
123	8	8	3		destination	Drag/drop from Flare Communicator Client
152	6	6	1		destination	CS 1000 Phone Range
17001	5	5	1		destination	Call Pilot DN of 7001
23	7	7	2		origination	5-digit ‘from’ header for CDR
911	3	3	0	1	destination	Emergency number

- Click **Commit**. The Adaptation Module defined for sample configuration is shown below.

**General**

\* Adaptation name: CS1KAdapt

Module name: CS1000Adapter

Module parameter: fromto=true

Egress URI Parameters:

Notes: Manipulate(Adapt) routing digits

**Digit Conversion for Incoming Calls to SM**

Add Remove

0 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
* 123	* 8	* 8		* 3		destination		drag/drop from SIP client
* 152	* 6	* 6		* 1		destination		CS1K station range
* 17001	* 5	* 5		* 1		destination		Call Pilot ACD DN
* 23	* 7	* 7		* 2		origination		CDR of 5-digits
* 911	* 3	* 3		* 0	1	destination		Emergency #

**Digit Conversion for Outgoing Calls from SM**

Add Remove

5 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
* 123	* 8	* 8		* 3		destination		drag/drop from SIP client
* 152	* 6	* 6		* 1		destination		CS1K station range
* 17001	* 5	* 5		* 1		destination		Call Pilot ACD DN
* 23	* 7	* 7		* 2		origination		CDR of 5-digits
* 911	* 3	* 3		* 0	1	destination		Emergency #

## 5.4. Define SIP Entities

A SIP Entity must be added for Communication Server 1000 and Communication Manager (5.4.1)

Expand **Elements - Routing** and select **SIP Entities** from the left navigation menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter an identifier for the SIP Entity ,  
“CS1000-Node 1006”
- **FQDN or IP Address:** “Node” IP address of the CS1000 IP Telephony interface  
“135.9.146.54”
- **Type:** Select “SIP Trunk”
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** Select the Adaptation Module defined above
- **Location:** Select the Location defined for Communication  
Server 1000 above.

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select “Use Session Manager Configuration”

Click **Commit** to save the definition of the new SIP Entity.

The following screen shows the SIP Entity defined for Communication Server 1000 in the sample configuration.

The screenshot displays the Avaya Aura System Manager 6.2 web interface. On the left, a navigation menu is expanded to 'Routing', with 'SIP Entities' selected. The main content area shows the 'SIP Entity Details' for 'CS1000-Node1006' in the 'General' tab. A red arrow points from a green box labeled 'CS1000 Node IP address' to the 'FQDN or IP Address' field, which contains '135.9.146.54'. Other fields include 'Name' (CS1000-Node1006), 'Type' (SIP Trunk), 'Notes' (empty), 'Adaptation' (CS1KAdapt), 'Location' (Westminster, CO, USA), and 'Time Zone' (America/Denver).

A second SIP Entity is required for the Communication Server 1000. This Entity will be associated with the TLS link required to send presence updates from the Communication Server 1000. The name will be different than the first Entity created above and no adaptation will be applied.

#### SIP Entity Details

##### General

* Name:	<input type="text" value="cs1k presence"/>
* FQDN or IP Address:	<input type="text" value="135.9.146.54"/>
Type:	<input type="text" value="SIP Trunk"/>
Notes:	<input type="text" value="Entity used for Presence"/>
Adaptation:	<input type="text" value=""/>
Location:	<input type="text" value="CS1K"/>
Time Zone:	<input type="text" value="America/Denver"/>
Override Port & Transport with DNS SRV:	<input type="checkbox"/>
* SIP Timer B/F (in seconds):	<input type="text" value="4"/>
Credential name:	<input type="text" value=""/>
Call Detail Recording:	<input type="text" value="egress"/>

##### SIP Link Monitoring

SIP Link Monitoring:

### 6.4.1 SIP Entity for Communication Manager

The SIP Entity built during the installation of the Midsize Enterprise (ME) server is required for Collaboration clients to access Communication Manager for features and is dedicated to that IMS (IP Multimedia Subsystem) functionality. A second SIP Entity is built for Communication Manager to handle Enterprise traffic (calls to/from Communication Server 1000 and calls to PSTN via Communication Server 1000). This Entity will have the same IP address as the SIP Entity built during the ME server installation. The corresponding Entity Link (5.5.1) however, will use a different TCP port and therefore a different Communication Manager SIP trunk than the SIP Entity and Entity Link built during the ME server install. This is done to ensure that Enterprise traffic can be handled separately from Collaboration client feature verification traffic and so that adaptations applied to Enterprise calling do not interfere with the IMS process. For the sample configuration, the second SIP Entity is named “gmi-alpha-cm-enterprise”.

Note: This Entity will have the Communication Manager adaptation applied whereas the Entity built during the ME server installation will not have an adaptation applied.

## SIP Entity Details

### General

* Name:	<input type="text" value="gmi-alpha-cm-enterprise"/>
* FQDN or IP Address:	<input type="text" value="135.9.146.130"/>
Type:	<input type="text" value="CM"/>
Notes:	<input type="text" value="For PCA &amp; PSTN calls"/>
Adaptation:	<input type="text" value="CM adaptation"/>
Location:	<input type="text" value="Westminster"/>
Time Zone:	<input type="text" value="America/Fortaleza"/>
Override Port & Transport with DNS SRV:	<input type="checkbox"/>
* SIP Timer B/F (in seconds):	<input type="text" value="4"/>
Credential name:	<input type="text"/>
Call Detail Recording:	<input type="text" value="none"/>

### SIP Link Monitoring

SIP Link Monitoring:	<input type="text" value="Use Session Manager Configuration"/>
Supports Call Admission Control:	<input type="checkbox"/>
Shared Bandwidth Manager:	<input type="checkbox"/>

## 5.5. Define Entity Links

Any connections to Session Manager are described by an Entity Link. In the sample configuration there will be two Entity Links between Session Manager and Communication Server 1000, one for MWI/Voice traffic and one for Presence Services. Likewise, two Entity links are required between Session Manager and Communication Manager, one for Collaboration client IMS services (created during the ME server installation) and one for communication with the Communication Server 1000.

### 5.5.1. Entity Links Communication Server 1000

The SIP trunk between Session Manager and Communication Server 1000 is described by an Entity link.

Expand **Elements** → **Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values.

- **Name** Enter an identifier for the link to each telephony system.
- **SIP Entity 1** Select SIP Entity defined for Session Manager
- **SIP Entity 2** Select the SIP Entity defined for Communication Server

- **Protocol** 1000 for voice calls in **Section 5.4**  
After selecting both SIP Entities, select “**TCP**” as the required protocol.
- **Port** Verify **Port** for both SIP entities is the default listen port.  
The default listen port is “**5060**”. Example uses TLS **5061**
- **Trusted** Enter ☒
- **Notes** Enter a brief description. [Optional]

Click **Commit** to save **Entity Link** definition.

The following screen shows the entity link defined for the SIP trunk between Session Manager and Communication Server 1000 for MWI and voice traffic.

Home / Elements / Routing / Entity Links

Entity Links

1 Item Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* SM to CS1K	* gmi-alpha-sm	TCP	* 5060	* CS1000-Node1000	* 5060	Trusted

The Entity Link for Presence services will use the Entity built for Communication Server 1000 Presence in Section 5.4 and will used TLS on port 5061.

Entity Links Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* sm-cs1k-tls	* gmi-alpha-sm	TLS	* 5061	* cs1k presence	* 5061	Trusted	CS1K Presence

### 5.5.2. Entity Link for Communication Manager

The Entity Link built between Session Manager and Communication Manager during the installation of the ME server is required for the Collaboration clients to access the Communication Manager for telephony features. A second Entity Link is built between Session Manager and Communication Manager to handle Enterprise traffic (calls to/from Communication Server 1000 and calls to PSTN via Communication Server 1000). This link will use a TCP port other than that used for the Entity Link built during the ME server installation. Using a different port requires a second SIP trunk to be built in Communication Manager and ensures that any inbound or outbound digit manipulation does not affect the IMS traffic required by the Collaboration clients to function properly.

1 Item   Refresh		Filter: Enable					
ame	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
sm-cm-top 5062	* gmi-alpha-sm	TCP	* 5062	* gmi-alpha-cm-enterprise	* 5062	Trusted	PCA&Enterprise calls

## 5.6. Define Routing Policy

Routing policies describe the conditions under which calls will be routed to Communication Server 1000 from either SIP endpoint registered to Session Manager. Routing Policies will also be used to send calls and Callpilot MWI notification messages from the Communication Server 1000 to the Avaya Communication Manager.

To add a routing policy, Expand **Elements - Routing** and select **Routing Policies**.

Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier to define the routing policy
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional]

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with Communication Server 1000 as defined above and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page.

Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

**Note:** The routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

The following screen shows the Routing Policy for Communication Server 1000.

Routing Policy Details

General

\* Name: to CS1000\_Node1006

Disabled: ☐

\* Retries: 0

Notes: CS1000 in Westminster, CO, USA

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
cs1k	135.9.146.54	SIP Trunk	Entity used for voice calls

Following the same procedure as above, a Routing Policy is built to Communication Manager. This is shown in the following screen:

Routing Policy Details

Commit | Cancel

General

\* Name: CM PCA Policy

Disabled: ☐

\* Retries: 0

Notes: Routing of PCA 555 calls

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
gmi-alpha-cm-enterprise	135.9.146.130	CM	For PCA calls

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Ranking	1 ▲	Name	2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0		24/7		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

## 5.7. Define Dial Pattern

Dial patterns are used to route calls to appropriate SIP Entities. In the sample configuration, since stations on Communication Server 1000 were assigned extensions starting with “52###”, calls starting with digits “52” will be routed to Communication Server 1000. Other Dial Patterns are also required for PSTN bound traffic, Communication Server 1000 traffic, MWI Notification and emergency dialing.

To define a dial pattern, expand **Elements - Routing** and select **Dial Patterns** (not shown).

Click **New**, (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls to Communication Server 1000
- **Min:** Enter the minimum number digits that must to be dialed.
- **Max:** Enter the maximum number digits that may be dialed.
- **SIP Domain:** Select the SIP Domain from drop-down menu or select “All” if Session Manager should accept incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional]

In the **Originating Locations and Routing Policies** section, click **Add**.

The **Originating Locations and Routing Policy List** page opens (not shown).

- In **Originating Locations** table, select “ALL”

- In **Routing Policies** table, select the Routing Policy that should be used to reoute the digits.
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Click **Commit** to save. The following screen shows the Dial Pattern defined for sample configuration. Since all calls bound for the Communication Server 1000 or PSTN via Communication Server 1000 will have a leading ‘1’ inserted, the dial pattern for those calls is simplified into a single entry.

Dial Pattern Details

CommitCancel

General

\* Pattern:1

\* Min:5

\* Max:12

Emergency Call:☐

Emergency Priority:1

Emergency Type:

SIP Domain:-ALL-

Notes:All calls to CS1k

Originating Locations and Routing Policies

AddRemove

1 Item RefreshFilter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Westminster	Auto Location	to CS1K	0	<input type="checkbox"/>	cs1k	

And the final dial pattern configuration is below:

Dial Patterns

EditNewDuplicateDeleteMore Actions

4 Items RefreshFilter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	1	5	12	<input type="checkbox"/>			-ALL-	All calls to CS1k
<input type="checkbox"/>	23	7	7	<input type="checkbox"/>			-ALL-	MWI Notify Messages for One-X Mobile
<input type="checkbox"/>	555	10	10	<input type="checkbox"/>			-ALL-	PCA Calls to SIP Clients
<input type="checkbox"/>	911	3	3	<input checked="" type="checkbox"/>	911	1	-ALL-	Emergency

The dial pattern ‘1’ is used to route PSTN bound calls as well as “drag and drop spotlight calls” from Flare Communicator client, 5-digit station calls and calls to CallPilot voicemail. The dial pattern ‘23’ is used for MWI notifications back to the Collaboration clients. The dial pattern ‘555’ is used for the routing of calls from Communication Server 1000 PCA calls. The routing digits used for PCA calls are arbitrary, however it is required that routing digits be used.

CT  
062012

©2012 Avaya Inc. All Rights Reserved.

48 of 101  
CollabPackCS1000.doc



It is necessary to route the MWI notifications differently than the PCA calls due to the requirement for Communication Manager to handle them differently. PCA calls will be routed to ARS digit-conversion and the MWI Notify messages will not.

Summary of Dial Patterns Used in this sample configuration are:

Pattern	Min	Max	SIP Domain	Emer.	Originating Location	Routing Policy	Notes
1	8	11	-ALL-	N	Westminster	to CS1K	All non-5 digit calls to CS1k
23	7	7	-ALL-	N	CS1K	CM Policy	MWI Notify Messages for One-X Mobile
555	10	10	-ALL-	N	CS1K	CM PCA Policy	PCA Calls to SIP Clients
911	3	3	-All-	Y	Westminster	to CS1K	Emergency Calls

## 6. Configure Avaya Aura® Communication Manager

This section describes the concepts needed to configure Communication Manager to support Converged endpoints for Communication Server 1000 with Avaya Aura® Midsize Enterprise. These instructions assume the Avaya G430 Gateway is already configured on Communication Manager. For information on how to administer other aspects of Communication Manager, see **References [14] and [15] in Section 12.**

The following administration steps will be described:

- Verify System Access codes match
- Verify - IP Network Region – SIP Domain
- Enable Trunk to Trunk transfers
- Administer Private, Public Numbering Plan and Uniform Dial plan
- Administer AAR/ARS Analysis
- Administer Dial Plan Analysis
- Administer Dial Plan Parameters
- Administer a Route Pattern
- Administer a SIP Trunk/Signal Group
- Administer Incoming Call Handling

### 6.1. Verify System Access Codes match

To allow users to utilize Converged dialing plans to route calls, verify the Communication Manager AAR and ARS access codes match Communication Server 1000 Access Codes.

Verify Communication Server 1000 Access Codes:

Navigate to **UCM Services – EM – ESN – ESN Access Codes and Parameters**

Managing: [135.9.139.206](#) Username: admin  
Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) » Customer 00 » Network Control & Services » ESN Access Codes and Basic Parameters

---

#### ESN Access Codes and Basic Parameters

##### General Properties

NARS/BARS Access Code 1:   
NARS Access Code 2:

NARS/BARS Dial Tone after dialing AC1 or AC2 access codes: ☒

In the **Dialplan Analysis** change your dialed string to match Feature Access Code (FAC) examples “9” and “6”.

## Using SMGR-Elements-Communication Manager-System-Dialplan Analysis

- Dialed String 6
- Total Length 1
- Call Type FAC—identifies this 1-digit number as a Feature Access Code
- Repeat steps to add digit '9' as FAC

Home / Elements / Communication Manager / System / Dialplan Analysis

gmi-alpha-cm

change dialplan analysis

Info:

change dialplan analysis
Page 1 of 12

DIAL PLAN ANALYSIS TABLE
Location: all Percent Full: 2

Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	1	attd						
15	8	ext						
19	7	ext						
2	7	ext						
3	7	ext						
4	7	ext						
5	5	ext						
6	1	fac						
7	7	ext						
8	7	ext						
9	1	fac						
*	3	dac						
#	3	dac						

Using SMGR-Elements-Communication Manager-System-Feature Access Codes  
On page 2 of Feature Access Codes, verify '9' is defined as ARSFAC1

#### Feature Access Codes List

[View](#) [Edit](#) [New](#)

36 Items   <a href="#">Refresh</a>   Show <span>15</span> <a href="#">▼</a>			Filter: <a href="#">Enable</a>
	Feature Access Code	Description	System
<input type="radio"/>	#51	Enhanced EC500 Deactivation	gmi-alphame-cm
<input type="radio"/>	*51	Enhanced EC500 Activation	gmi-alphame-cm
<input type="radio"/>	*50	EC500 Self-Administration AC	gmi-alphame-cm
<input type="radio"/>	*61	Directed Call Pickup AC	gmi-alphame-cm
<input type="radio"/>	#80	Contact Closure Close Code	gmi-alphame-cm
<input type="radio"/>	*80	Contact Closure Open Code	gmi-alphame-cm
<input type="radio"/>	*42	CAS Remote Hold/Answer Hold-Unhold AC	gmi-alphame-cm
<input type="radio"/>	*41	CCall Pickup Access Code	gmi-alphame-cm
<input type="radio"/>	*40	Call Park Access Code	gmi-alphame-cm
<input type="radio"/>	#30	Call Forwarding Deactivation	gmi-alphame-cm
<input type="radio"/>	*31	Call Forwarding Activation	gmi-alphame-cm
<input type="radio"/>	*30	Call Forwarding Activation Busy/DA	gmi-alphame-cm
<input type="radio"/>	#33	Automatic CallBack Deactivation	gmi-alphame-cm
<input type="radio"/>	*33	Automatic CallBack Activation	gmi-alphame-cm
<input type="radio"/>	9	ARSFAC1	gmi-alphame-cm

On page 3 of Feature Access Codes, select AARFAC and choose 'Edit'  
Add '6' in Auto Alternate Routing Field

change feature-access-codes

Page 1 of 10

FEATURE ACCESS CODE (FAC)

Abbreviated Dialing List1

Access Code:

\*10

Abbreviated Dialing List2

Access Code:

\*12

Abbreviated Dialing List3

Access Code:

\*13

Abbreviated Dial - Prgm Group List

Access Code:

\*14

Announcement

Access Code:

\*19

Answer Back

Access Code:

Auto Alternate Routing (AAR)

Access Code:

6

Navigating to System Manager-Elements-Communication Manager-System-Dialplan Parameters

Select the item and choose 'Edit':

UDP Extension Search Order      udp-table-first

gmi-alphame-cm

change dialplan parameters

Enter

Refresh

Cancel

Clear Field

Help

Edit

Prev Page

Next Page

Info:

change dialplan parameters

Page 1 of 1

#### DIAL PLAN PARAMETERS

Local Node Number:

ETA Node Number:

UDP-ARS Calls Considered Offnet?

ETA Routing Pattern:

UDP Extension Search Order:

udp-table-first

## 6.2. Verify IP Network Region - Domain

Navigate to **Elements – Communication Manager – Network** and Select the **Network Region**. Enter the following values and use default values for remaining fields.

- **Authoritative Domain:** Enter the correct SIP domain for the configuration. For the reference configuration, “**us.global.avaya.com**” was used.
- **Name:** Enter descriptive name.

gmi-alphame-cm

display ip-network-region 1



Info:

display ip-network-region 1		Pa
IP NETWORK REGION		
Region:	1	
Location:	1	Authoritative Domain: us.global.avaya.com
Name: LOCAL		

### 6.3. Configure Trunk-to-Trunk Transfers

Use the **change system-parameters features** command to enable trunk-to-trunk transfers. This feature is needed when an incoming call to a SIP station is transferred to another SIP station. For simplicity, the **Trunk-to-Trunk Transfer** field on **Page 1** was set to “all” to enable all trunk-to-trunk transfers on a system wide basis.

**Note:** Enabling this feature poses significant security risk by increasing the risk of toll fraud, and must be used with caution. To minimize the risk, a COS could be defined to allow trunk-to-trunk transfers for specific trunk group(s). For more information regarding how to configure Communication Manager to minimize toll fraud, see **Reference [16]** in **Section 12**.

Navigate to **Elements – Communication Manager – Parameters-System Parameters – Features**.

Select “**True**”.

## System Parameters - Features

Select device(s) from Communication Manager List ▶

### System Parameters - Features List

[View](#) [Edit](#) [New](#)

1 Item | Refresh | Show [ALL](#) ▼

	Terminal Translation Initialization (TTI) Enabled	EMU Inactivity Interval for Deactivation(hours)
	true	

Select edit,  
choose“all”.

Home / Elements / Communication Manager / Parameters / System Parameters - Features

**gmi-alphame-cm**

change system-parameters features

[Enter](#) [Refresh](#) [Cancel](#) [Clear Field](#) [Help](#) [Edit](#) [Prev](#)

Info: Select suggested values from dropdown

change system-parameters features		Page 1
FEATURE-RELATED SYSTEM PARAMETERS		
Self Station Display Enabled?		<input type="text" value="y"/>
Trunk-to-Trunk Transfer:		<input type="text" value="all"/>
Automatic Callback with Called Party Queuing?		<div>all none restricted</div>
Automatic Callback - No Answer Timeout Interval (rings):		<div>&lt; 10 &gt;</div>
Call Park Timeout Interval (minutes):		<input type="text" value="10"/>
Off-Premises Tone Detect Timeout Interval (seconds):		<input type="text" value="20"/>
AAR/ARS Dial Tone Required?		<input type="text" value="y"/>

## 6.4. Administer Signal Group

Signal Group 4 and the associated SIP Trunk Group 4 will be used for all traffic to the Communication Server 100.

Navigate to System Manager-Elements-Communication Manager-Network-Signaling Groups-Select New

- Qualifier “4” This is the signal group number, select Add
- Group Type SIP
- Transport Method TCP—alternatively, TLS can be used
- Near-End Node Name procr—this name is created during the ME server install
- Far-End Node Name SM—this name is created during the ME server install
- Near-End Listen Port 5062—needs to be a different port than signal group 3
- Far-End Listen Port 5062—needs to be a different port than signal group 3
- Far-End Network Region 1
- Domain us.global.avaya.com—replace with SIP domain

Signal Group form should appear as below:

change signaling-group 4 Page 1 of 2

**SIGNALING GROUP**

Group Number: 4	Group Type: sip	
IMS Enabled? <input type="checkbox"/>	Transport Method: <input type="text" value="tcp"/>	
Q-SIP? <input type="checkbox"/>		
IP Video? <input type="checkbox"/>	Enforce SIPS URI for SRTP? <input type="checkbox"/>	
Peer Detection Enabled? <input type="checkbox"/>	Peer Server: SM	

Near-end Node Name: <input type="text" value="procr"/>	Far-end Node Name: <input type="text" value="SM"/>
Near-end Listen Port: <input type="text" value="5062"/>	Far-end Listen Port: <input type="text" value="5062"/>
	Far-end Network Region: <input type="text" value="1"/>
Far-end Domain: <input type="text" value="us.global.avaya.com"/>	

Incoming Dialog Loopbacks: <input type="text" value="eliminate"/>	Bypass If IP Threshold Exceeded? <input type="checkbox"/>
DTMF over IP: <input type="text" value="rtp-payload"/>	RFC 3389 Comfort Noise? <input type="checkbox"/>
Session Establishment Timer(min): <input type="text" value="3"/>	Direct IP-IP Audio Connections? <input type="checkbox"/>
Enable Layer 3 Test? <input type="checkbox"/>	IP Audio Hairpinning? <input type="checkbox"/>
H.323 Station Outgoing Direct Media? <input type="checkbox"/>	Initial IP-IP Direct Media? <input type="checkbox"/>
	Alternate Route Timer(sec): <input type="text" value="6"/>



Select Enter.

## 6.5. Administer SIP Trunk Group

Trunk Group 4 will use signal group 4 created in section 6.4 and will be used for all traffic to the Communication Server 1000.

Navigate to System Manager-Elements-Communication Manager-Network-Trunk Group- Select New

- Qualifier “4” This is the trunk group number, select Add
- Group Type SIP
- Group Name free text up to 27 characters (‘To CS1K’ in this config)
- TAC \*04—this is the trunk access code
- Service Type TIE
- Assignment Method auto
- Signal Group 4—signal group number created in section 7.4
- Number of Members 50

Trunk Group form should appear as below:

change trunk-group 4

Info: Enter number between 0-255

change trunk-group 4

Page 1 of 21

TRUNK GROUP

Group Number: 4

Group Type: sip

CDR Reports: y

Group Name: To CS1K

COR: 1

TN: 1

TAC: \*04

Direction: two-way

Outgoing Display? n

Dial Access? n

Night Service:

Queue Length: 0

Service Type: tie

Auth Code? n

Member Assignment Method: auto

Signaling Group: 4

Number of Members: 100

Select Enter.

## 6.6. Verify Signal Group and Trunk Group are In-Service

After Signal Group 4 and Trunk Group 4 have been added, ensure that both are up and in-service.

Navigating to System Manager-Elements-Inventory-Synchronization-Communication System-  
-Launch Element Cut Through

Type 'status signaling-group 4'

Results should be as below "in-service"

### Element Cut Through

[Done](#)

---

**gmi-alphame-cm**

Command:  [Send](#)

[Enter](#) [Refresh](#) [Cancel](#) [Clear Field](#) [Help](#) [Edit](#) [Prev Page](#) [Next Page](#) [More Actions](#)

Info:

**status signaling-group 4**

**STATUS SIGNALING GROUP**

Group ID: 4

Group Type: sip

**Group State: in-service**

Type 'status trunk 4'

Results should be as below 'in-service/idle' and 'Mtce Busy = no' for all 100 members (use Next Page to verify)

## Element Cut Through

Done

gmi-alphame-cm

Command:

Info: Command successfully completed

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0004/043	T00298	in-service/idle	no
0004/044	T00299	in-service/idle	no
0004/045	T00300	in-service/idle	no

## 6.7. Configure Incoming Call Handling for Trunk Group

In order to strip the routing digits of '555' for PCA calls from the Communication Server 1000 to Collaboration clients, an Incoming Call Handling Rule is needed on the trunk group in Communication Manager. The Insert of '9' will route the call to ARS where ARS digit-conversion will keep it local rather than looping back to the Communication Server 1000.

Navigating to System Manager-Elements-Inventory-Synchronization-Communication System--Launch Element Cut Through

Type "change incoming tru 4"

- **Number Len**            **10**
- **Number Digits**       **555**
- **Del**                      **3**
- **Insert**                  **9**

Command: 

Info:

change inc-call-handling-trmt trunk-group 4

Page 1 of 30

## INCOMING CALL HANDLING TREATMENT

Service/ Feature	Number Len	Number Digits	Del	Insert
tie	10	555	3	9
tie				
tie				

## 6.8. Verify IP Network Region - Domain

Use the **change ip-network-region n** command where **n** is an available network region.

Enter the following values and use default values for remaining fields.

- Authoritative Domain:** Enter the correct SIP domain for the configuration.  
 For the sample configuration, “**us.global.avaya.com**” was used.
- Name:** Enter descriptive name.
- Codec Set:** Enter the number of the IP codec set 1 above
- Intra-region IP-IP Direct Audio:** Enter “yes”.
- Inter-region IP-IP Direct Audio:** Enter “yes”.

gmi-alphame-cm

display ip-network-region 1



Info:

**display ip-network-region 1** Pa

**IP NETWORK REGION**

Region: 1	
Location: 1	Authoritative Domain: <span style="border: 2px solid red; padding: 2px;">us.global.avaya.com</span>
Name: LOCAL	

## 6.9. Administer Private Numbering Plan (

The full extension numbers used for the collaboration clients registered to Session Manager must be added to the private numbering table on Communication Manager. For the reference configuration, private numbering was used and all extension numbers were unique within the private network. However, in many customer networks, it may not be possible to define unique extension numbers for all users within the private network. For these types of networks, additional administration may be required as described in **Reference [14]** in **Section 12**. Use the **change private-numbering n** command, where **n** is the length of the private number. Fill in the indicated fields as shown below.

- **Ext Len:** Enter length of extension numbers.  
In the sample configuration, “7” was used.
- **Ext Code:** Enter leading digit (s) from extension number.  
In the sample configuration, “235xxxx” were used for SIP endpoints.
- **Trk Grp(s):** Enter trunk groups or leave blank to use format on all trunk groups
- **Private Prefix:** Leave blank unless an enterprise canonical numbering scheme is

- **Total Length:** Enter “7” since a private prefix was not defined.

change private-numbering 7					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
7	23	3		7	Total Administered: 3

## 6.10. Administer Public Numbering Plan

The full extension numbers used for the collaboration clients registered to Session Manager must be added to the public numbering table on Communication Manager. For the sample configuration, public numbering was used and all extension numbers were unique within the public network. However, in many customer networks, it may not be possible to define unique extension numbers for all users within the private network. For these types of networks, additional administration may be required as described in **Reference [14] in Section 12.**

Use the **change public-numbering n** command, where **n** is the length of the number.

Fill in the indicated fields as shown below.

- **Ext Len:** Enter length of extension numbers.  
In the sample configuration, “7” was used.
- **Ext Code:** Enter leading digit (s) from extension number.  
In the sample configuration, “235xxxx” were used for SIP endpoints.
- **Trk Grp(s):** Enter trunk groups or leave blank to apply for all trunks.
- **Public Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix.
- **Total Length:** Enter “5” since a private prefix was not defined.

These settings will ensure that a 7-digit station will show a 5-digit Calling Party Number (CPN) on outbound calls. For example, SIP extension “2352001” will show a Calling Party Number of “52001”.

change public-unknown-numbering 7					Page 1 of 2
NUMBERING - PUBLIC FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Public Ukn Prefix	Total Len	
7	2	4	1303	5	Total Administered: 1

## 6.11. Administer Uniform Dial Plan

Navigate to **Elements – Communication Manager – System – Uniform Dial Plan** and add dialing plan extension range (s). In the reference configuration, 7-digit extension numbers starting with “**235xxxx**” was used for the collaboration clients associated and **52xxx** is used as the uniform dialing plan for Converged Users dialing across Communication Server and the Collab Pack.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Matching Pattern** Enter digit pattern of extensions assigned to SIP endpoints (Collaboration clients) and Communication Server 1000 endpoints.
- **Len** Enter extension length.
- **Net** Enter “**ars**”.

Navigate to **Elements – CM –System – Uniform Dial Plan**.

Home / Elements / Communication Manager / System / Uniform Dial Plan

### Uniform Dial Plan

Select device(s) from Communication Manager List ▶

---

#### Uniform Dial Plan List

3 Items | Refresh | Show

	Matching Pattern	Length	Del	Insert Digits	Net
<input type="radio"/>	52	5	0		ars

The above example is for the Communication Server 1000 station range. Following the same procedure as above, add an entry that represents the pattern range for the SIP clients (**23xxx** in this sample configuration) and the CallPilot access number (**7001**) as in this sample configuration..

The completed Uniform Dial Plan Table is represented in the following screen:

### Uniform Dial Plan List

[View](#) [Edit](#) [New](#)

3 Items   <a href="#">Refresh</a>   Show <span>ALL</span>			Filter: <a href="#">Enable</a>					
	Matching Pattern	Length	Del	Insert Digits	Net	Conv	Node Number	System
<input type="radio"/>	7001	4	0		ars	false		gmi-alphame-cm
<input type="radio"/>	52	5	0		ars	false		gmi-alphame-cm
<input type="radio"/>	23	7	0		ars	false		gmi-alphame-cm
Select : <a href="#">None</a>								

## 6.12. Administer Route Pattern

This section provides the configuration of the Route Pattern used in Communication Manager for the routing of calls to the Communication Server 1000, Call Pilot and PSTN via Communication Server 1000. All calls from ARS will use this route pattern 4. Route Pattern 3 is created during the ME server installation and is dedicated for the IMS signaling required by the Collaboration clients. Using a separate route pattern (route pattern 4 in this sample configuration) allows for digit manipulation on enterprise calls without affecting the IMS traffic that is using Route Pattern 3.

Navigating to System Manager-Elements-Communication Manager-Network-Route Pattern-Select New

- Qualifier “4” This will be the route pattern number
- Name Free-text up to 15 characters (To CS1K in this sample configuration)
- Grp No “4” This is the trunk group number to be used for this route
- Inserted Digits “1” Lead routing digit that SM will use to point the call to CS1K
- FRL “0” The minimal facility access code restriction



change route-pattern 4

Info:

change route-pattern 4 Page 1 of 3

Pattern Number: 4 Pattern Name:

SCCAN?  Secure SIP?

Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/	IXC
No	Mrk	Lmt	List	Del	Dgts			QSIG	
								Intw	
1:	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="n"/>	<input type="text" value="user"/>
2:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="n"/>	<input type="text" value="user"/>
3:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="n"/>	<input type="text" value="user"/>
4:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="n"/>	<input type="text" value="user"/>
5:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="n"/>	<input type="text" value="user"/>
6:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="n"/>	<input type="text" value="user"/>

## 6.13. Administer ARS Analysis

This section provides the configuration of the ARS pattern used in the reference configuration for routing calls between collaboration clients and Communication Server 1000 stations, Call Pilot and to the PSTN via Communication Server 1000. All traffic that is bound for the PSTN must have dialed strings defined here as well as any digit strings pointed to ARS via the UDP table in section 6.7 (23x-xxxx, 52xxx and 7001 for this sample configuration). The ARS table needs to mimic the dialing rules of the Communication Server 1000 including local, long distance, toll-free and emergency dialing. All dialed numbers identified on the ARS table will be sent to Session Manager and routed to the Communication Server 1000 via Route pattern 4 created in section 6.8.

e.g. **52001** is the 5-digit number of a Communication Server 1000 station

- **Dialed String** Enter leading digit (s) of extension numbers, “5”
- **Min** Enter minimum number of digits that must be dialed. “5”.
- **Max** Enter maximum number of digits that may be dialed. “5”
- **Route Pattern** Enter Route Pattern of “4”
- **Call Type** Enter “locl”.

The completed ARS table below describes a dialing plan that supports local 7-digit dialing, 1+10 long distance dialing and 1+10 toll-free dialing. Since the drag/drop calling feature from the contact fan of the Flare Communicator client will be dialing 7-digits to other SIP client users that is accounted for in the ARS table as well.

## Automatic Route Selection Analysis List

View Edit New

11 Items   Refresh   Show ALL						Filter: Enable
	Dialed String	Total Min	Total Max	Route Pattern	Location	System
<input type="radio"/>	1	11	11	4	all	gmi-alphame-cm
<input type="radio"/>	2	7	7	4	all	gmi-alphame-cm
<input type="radio"/>	3	7	7	4	all	gmi-alphame-cm
<input type="radio"/>	4	7	7	4	all	gmi-alphame-cm
<input type="radio"/>	5	7	7	4	all	gmi-alphame-cm
<input type="radio"/>	5	5	5	4	all	gmi-alphame-cm
<input type="radio"/>	6	7	7	4	all	gmi-alphame-cm
<input type="radio"/>	7001	4	4	4	all	gmi-alphame-cm
<input type="radio"/>	8	7	7	4	all	gmi-alphame-cm
<input type="radio"/>	9	7	7	4	all	gmi-alphame-cm
<input type="radio"/>	911	3	3	4	all	gmi-alphame-cm

## 6.14. Administer ARS Digit Conversion

This section provides the configuration of the ARS Digit-Conversion rule used in the sample configuration for keeping inbound 7-digit calls local rather than routing back out to the Communication Server 1000. In order to support drag/drop calling from the Flare Communicator client contact fan (which is a 7-digit call) to other Converged Users, changes were made to the dial plan parameters form (see section 6.1). The changes made to the Dial Plan Parameters form routed 7-digit traffic to the **23x-xxxx** range off-net so that a 7-digit call will ring the Communication Server station first (invoking PCA/SIMRING capability) rather than just the Collaboration Client that is being called. Without a rule to keep inbound 7-digit traffic local, PCA calls to 7-digit SIP clients would also be routed off-net creating a loop condition. Inbound 7-digit calls will be kept local by using an ARS Digit-Conversion rule that states the **23x-xxxx** range represents extensions. The Incoming-Call Handling rule created in section 6.7 is inserting the digit '9' which routes the call to ARS. Before ARS Analysis is invoked, ARS Digit-Conversion rules are applied.

Navigating to System Manager-Elements-Communication Manager-Network-Automatic Route Selection Digit Conversion:

- Matching Pattern      23 (leading digits of Collaboration clients)
- Min                      7 (length of Collaboration client extension)
- Max                      7 (length of Collaboration client extension)
- Del                      0 (no changes made to digit string)
- Net                      ext (defining this range as 'ext' prevents loop)
- Conv                    blank (no other conversion should be applied to this digit string)

Screen capture is below:

Edit ARS Digit Conversion

[Commit](#) [Reset](#) [Schedule](#) [Cancel](#)

System

Location

Percent Full

32 Items [Refresh](#)

Matching Pattern	Min	Max	Del	Replacement String	Net	Conv	ANI Required
<input type="text" value="23"/>	<input type="text" value="7"/>	<input type="text" value="7"/>	<input type="text" value="0"/>	<input type="text" value=""/>	<div>ext</div>	<input type="checkbox"/>	<div>n(o)</div>

## 7. Avaya Aura® Presence Services Configuration

This section provides the procedures to verify the configuration of Avaya Aura® Presence Services. Presence Services can support collaboration clients such as Avaya Flare Communicator on iPad and Avaya one-X Mobile SIP for iOS client registered as SIP endpoints to Avaya Aura® Session Manager, as well as telephony clients such as M3900 / 1100 / 1200 series phones on the Communication Server 1000.

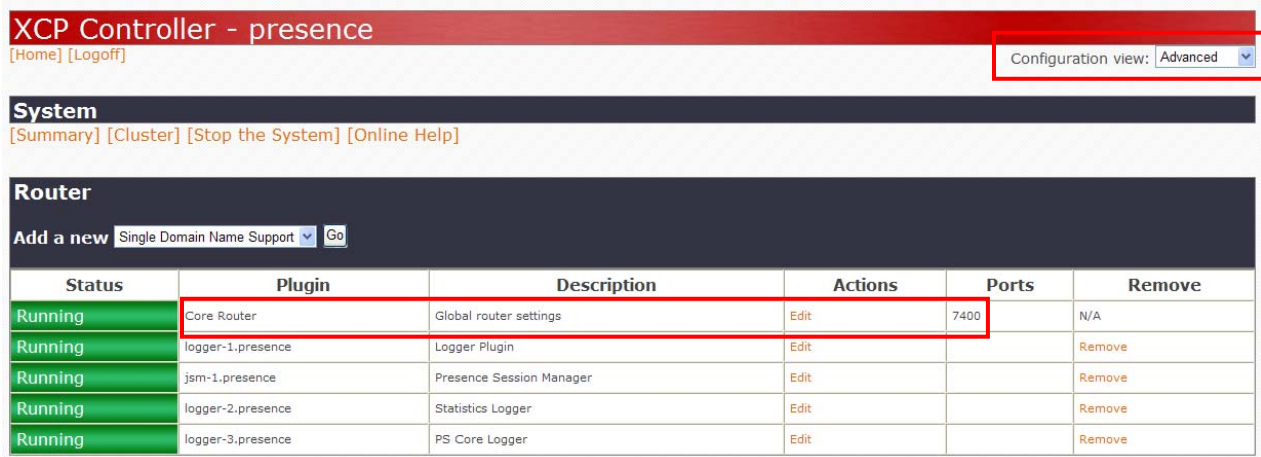
These instructions assume Presence Services has been installed and configured as described by **References [10] through [11] in Section 12**. For example, the configuration describing how Presence Services connects to several other elements in the network such as System Manager and Session Manager should be completed during installation. Therefore, this section will focus on verifying the configuration is correct.

Presence Services is configured using the browser-based **XCP Controller** graphical user interface. Access the **XCP Controller** interface using the URL “**https://<ip-address>:7300/admin**”, where “<ip-address>” is the IP address of the server running Avaya Aura® Presence Services software. Log-in with the appropriate credentials.

### 7.1. Verify Configuration of Trusted Hosts

**Step 1:** Select “**Advanced**” from the drop-down menu for the **Configuration view:** field on the top right hand corner to enter the Advanced configuration mode.

In the **Router** section, select the **Edit** link associated with the **Plugin** component named “**Core Router**” as shown below.



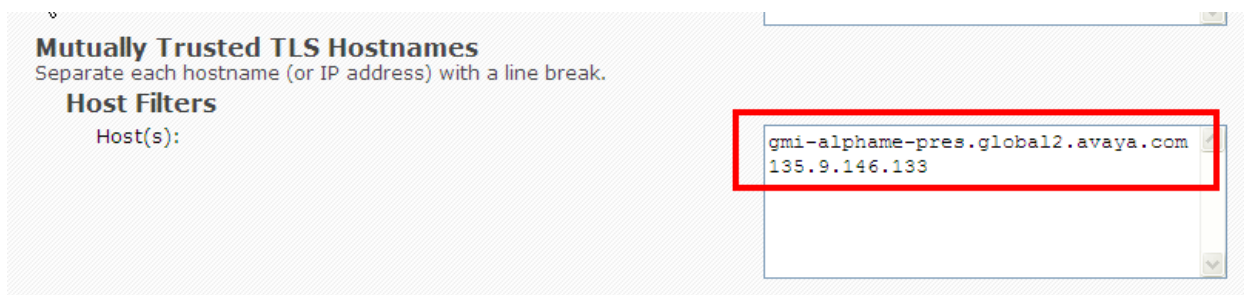
The screenshot shows the XCP Controller - presence web interface. At the top, there is a red header bar with the text "XCP Controller - presence" and links for "[Home]" and "[Logoff]". On the right side of the header, there is a "Configuration view:" dropdown menu set to "Advanced". Below the header, there is a "System" section with links for "[Summary]", "[Cluster]", "[Stop the System]", and "[Online Help]". The main section is titled "Router" and contains a table of plugins. The table has columns for Status, Plugin, Description, Actions, Ports, and Remove. The first row, "Core Router", is highlighted with a red border. The "Status" column for all rows shows "Running". The "Ports" column for the "Core Router" row shows "7400".

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.presence	Logger Plugin	Edit		Remove
Running	jsm-1.presence	Presence Session Manager	Edit		Remove
Running	logger-2.presence	Statistics Logger	Edit		Remove
Running	logger-3.presence	PS Core Logger	Edit		Remove

**Step 2:** On the **Global Settings Configuration** page (not shown), scroll down to the **Mutually Trusted TLS Hostnames** section and verify the Fully Qualified Host Name of the server running Presence Services software has already been added in the **Host(s):** field.

Verify IP addresses of SIP Signaling Interface of each Session Manager have also been entered in the same field.

For reference configuration, these values were “**gmi-alphame-pres.global2.avaya.com**”, **135.9.146.133**” as shown below.



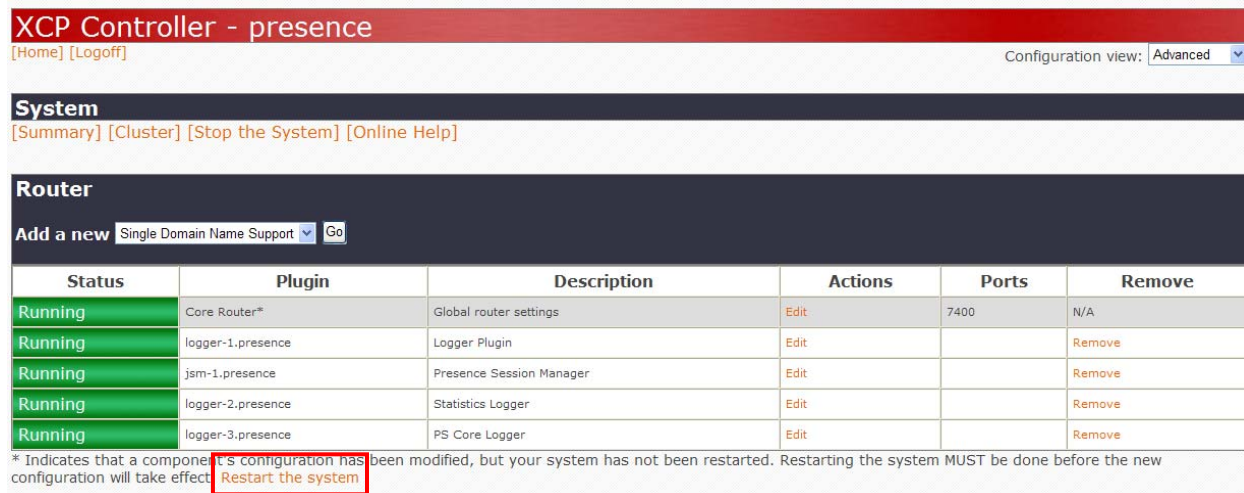
**Mutually Trusted TLS Hostnames**  
Separate each hostname (or IP address) with a line break.

**Host Filters**  
Host(s):

gmi-alphame-pres.global2.avaya.com  
135.9.146.133

Click **Submit** to save changes.

**Step 3:** Select the **Restart the system** link for the changes to take effect.



**XCP Controller - presence**  
[Home] [Logoff] Configuration view: Advanced

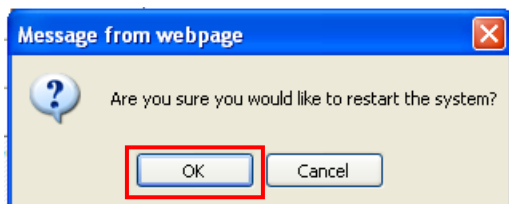
**System**  
[Summary] [Cluster] [Stop the System] [Online Help]

**Router**  
Add a new Single Domain Name Support Go

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router*	Global router settings	Edit	7400	N/A
Running	logger-1.presence	Logger Plugin	Edit		Remove
Running	jsm-1.presence	Presence Session Manager	Edit		Remove
Running	logger-2.presence	Statistics Logger	Edit		Remove
Running	logger-3.presence	PS Core Logger	Edit		Remove

\* Indicates that a component's configuration has been modified, but your system has not been restarted. Restarting the system MUST be done before the new configuration will take effect. **Restart the system**

Click **OK** in the system dialog.



**Step 4:** Refresh the browser to verify the **Status** of all system components returns to “**Running**” as shown below:

**Note:** the Restart operation may take several minutes to complete.

XCP Controller - presence
[Home] [Logout]
Configuration view: Advanced

System
[Summary] [Cluster] [Stop the System] [Online Help]

Router
Add a new Single Domain Name Support Go

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.presence	Logger Plugin	Edit		Remove
Running	sm-1.presence	Presence Session Manager	Edit		Remove
Running	logger-2.presence	Statistics Logger	Edit		Remove
Running	logger-3.presence	PS Core Logger	Edit		Remove

Components
Add a new Connection Manager Go

Status	Component	Description	Actions	Ports	Remove
Running	sip-ps-1.presence	SIP Presence Server	Edit, Stop	15061	N/A
Running	sip-proxy-1.presence	SIP Proxy	Edit, Stop	5061 5061 15061 25061	N/A
Running	sip-bulks-1.presence	SIP Bulk Subscription Server	Edit, Stop	25061	N/A
Running	cm-1.presence	Connection Manager	Edit, Stop	5222 5223 7400	N/A
Running	presence-container-1.presence	Presence Server	Edit, Stop		N/A
Running	presence_model-1.presence	Presence Transformer Component	Edit, Stop		N/A
Running	rims-1.presence	Resource List Management Service	Edit, Stop		N/A
Running	rims.presence	Generic Open Port	Edit, Stop		N/A
Running	idmapper-1.presence	IdMapper Component	Edit, Stop		N/A
Running	authzmanager-1.presence	Authz Component	Edit, Stop		N/A
Running	im-1.presence	IM Transcripts Component	Edit, Stop		N/A
Running	stanza-optimizer-1.presence	Stanza Optimizer Component (XEP-033)	Edit, Stop		N/A
Running	aes-collector-1.presence	AES Collector	Edit, Stop		N/A

## 7.2. Verify Configuration to support Avaya SIP Endpoints

**Step 1:** Select “**Advanced**” from the drop-down menu for the **Configuration view:** field on the top right hand corner to enter the Advanced configuration mode.

In the **Router** section, select the **Edit** link associated the **Plugin** component named “**Presence Session Manager**” as shown below.

XCP Controller - presence

[\[Home\]](#) [\[Logoff\]](#)

Configuration view: Advanced

System

[\[Summary\]](#) [\[Cluster\]](#) [\[Stop the System\]](#) [\[Online Help\]](#)

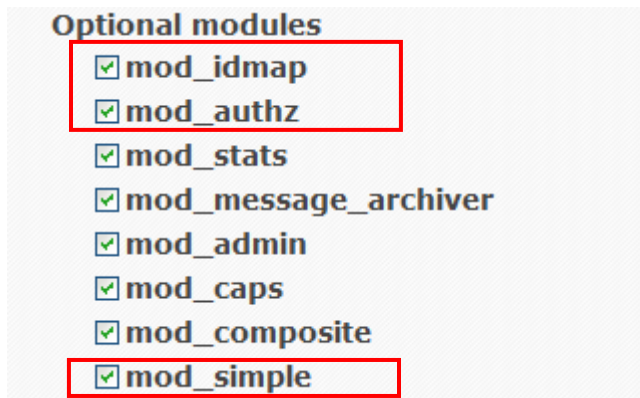
Router

Add a new Single Domain Name Support Go

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	<a href="#">Edit</a>	7400	N/A
Running	logger-1.presence	Logger Plugin	<a href="#">Edit</a>		<a href="#">Remove</a>
Running	psm-1.presence	Presence Session Manager	<a href="#">Edit</a>		<a href="#">Remove</a>
Running	logger-2.presence	Statistics Logger	<a href="#">Edit</a>		<a href="#">Remove</a>
Running	logger-3.presence	PS Core Logger	<a href="#">Edit</a>		<a href="#">Remove</a>

**Step 2:** On the **Presence Session Manager Configuration** page (not shown), scroll to the **Optional modules** section and verify the following modules have been selected as shown below.

- **mod\_idmap** Verify ☒ has been entered.
- **mod\_authz** Verify ☒ has been entered.
- **mod\_simple** Verify ☒ has been entered.

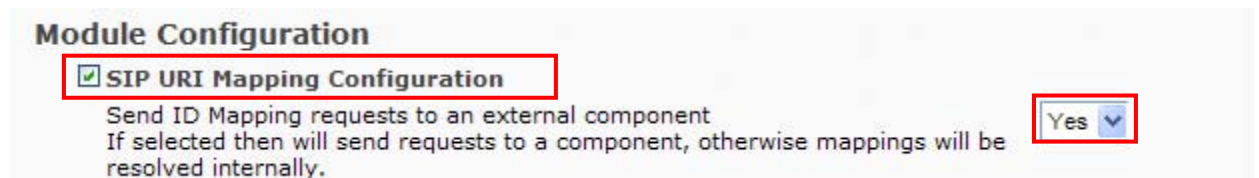


**Step 3:** Scroll down to the **Module Configuration** section and verify the following fields have been configured:

- **SIP URI Mapping Configuration** Verify ☒ has been entered.
- **Send ID Mapping requests to an external component**

Verify

“Yes” has been selected.



**Step 4:** Click **Submit** (not shown) to save changes.

**Step 5:** Select the **Restart the system** link (not shown) as described in the **Section 5.1**.



## 8. Configure CallPilot

The assumption is that Callpilot is already installed and configured with voicemail boxes setup for the Communication Server 1000 clients. Please refer to **Reference [17] in Section 12** for detailed documentation.

The following is required:

- Verify CallPilot Service DN fits with the Collaboration Pack dial plan (not shown)
- Verify NMS is enabled (not shown)
- Registering CallPilot with System Manager
- Add CallPilot certificate to System Manager

### 8.1. Registering CallPilot to the Element Registry

To be able to administer CallPilot via System Manager, CallPilot must be registered with System Manager.

Navigate to **UCM Services – Elements**- Select **Add**

- |  |  |
|--|--|
| • <b>Name:</b>                         | Specify the element name of the CallPilot, “ <b>CallPilot</b> ”.   |
| • <b>Description:</b>                  | Specify the element description of the CallPilot, “ <b>CallPilot</b> ”   |
| • <b>Type:</b>                         | Select the element type from the drop-down list.<br>On the Add New Element page, click <b>Next</b> and then specify the following: |
| • <b>CallPilot Manager address:</b>    | Specify the FQDN or IP address of the CallPilot Manager, “ <b>135.9.139.208</b> ”.   |
| • <b>CallPilot server address:</b>     | Specify the FQDN or IP address of the CallPilot server., “ <b>135.9.146.55</b> ”.  |
| • <b>Administrator mailbox number:</b> | Specify the administrator mailbox number. “ <b>000000</b> ”  |
| • <b>Administrator password:</b>       | Specify the administrator password. “ <b>123456</b> ”  |

Click **Save**.

Host Name: gmi-alphame-smgr.global2.avaya.com    Software Version: 02.20\_SMGR-SNAPSHOT(5167)    User Name admi

#### Add New Element

**Step1:** Identify the new element.

Enter a name and optional description. Depending on the selected element Type, additional steps may be required.

Name:	<input type="text" value="CallPilot"/>	(1-256 characters)
Description	<input type="text" value="CallPilot"/>	
Type:	<input type="text" value="CallPilot Messaging"/> ▼	

## Add New Element

Step2: Identify the element's management server in your network.

CallPilot Manager address:	<input type="text" value="135.9.139.208"/>
	FQDN or IP address
CallPilot server address:	<input type="text" value="135.9.146.55"/>
	FQDN or IP address
Administrator mailbox number:	<input type="text" value="000000"/>
Administrator password:	<input type="password" value="•••••"/>

## 8.2. Adding CallPilot certificate to System Manager

Navigate to **CallPilot Manager** secure URL and save the .cer file to desktop. For the reference configuration this is “**https:// 135.9.139.208/cpmgr**”.

Navigate on the System Manager Web Console, to **Elements- Inventory – Manage Elements**

In the **Elements** section, select a managed element instance, “**System Manager 6.2**”.

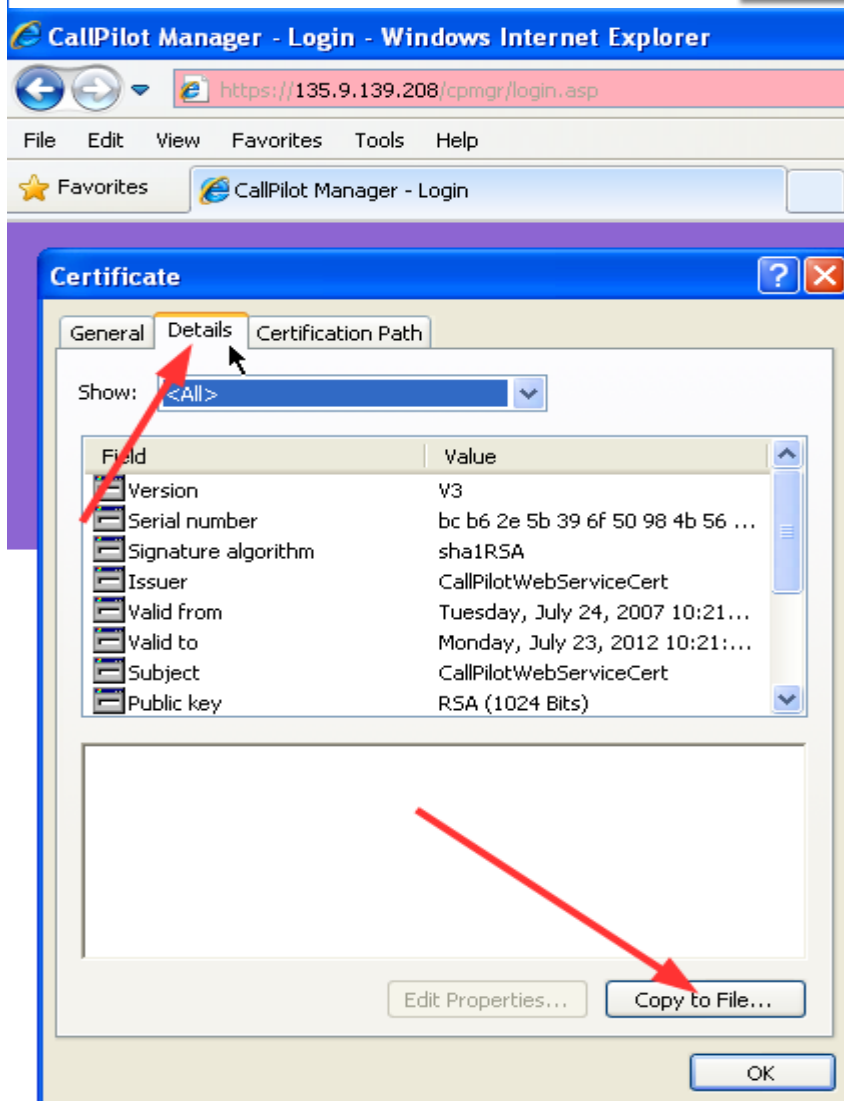
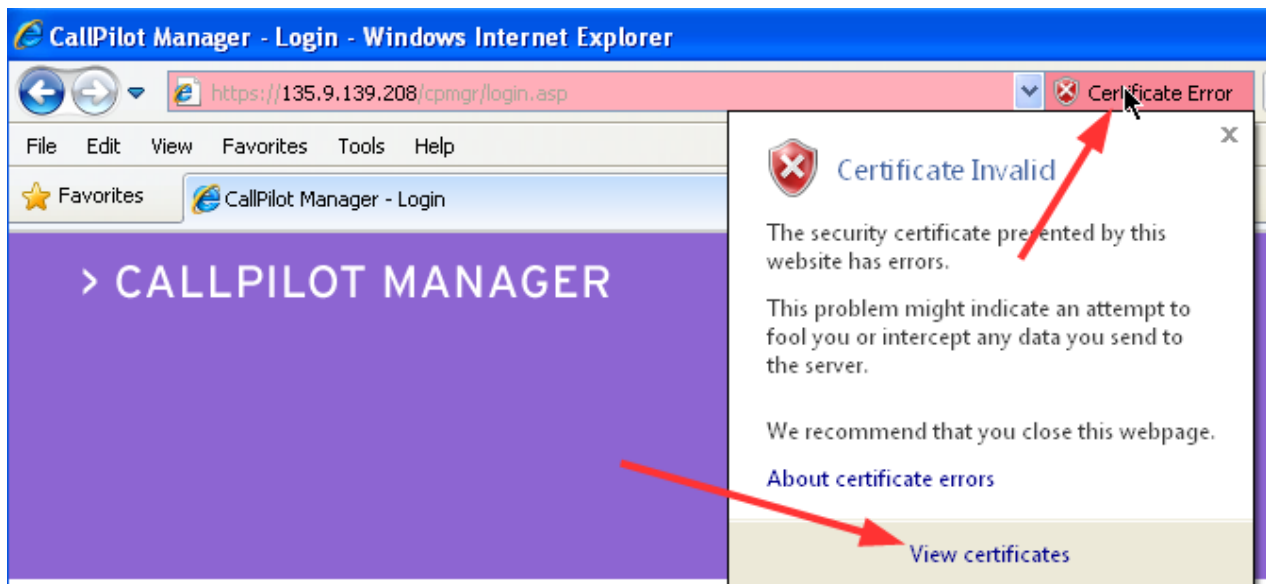
Select **More Actions - Configure Trusted Certificates**.

The system displays the certificates that are currently installed on the managed Element selected.

To add a CallPilot certificate, click **Add**. On the Add Trusted Certificate page, in the **Select Store Type to add trusted certificate** field, click **All**.

To add the certificate, Import the certificate by selecting “**Import from File**”.

Click “**Commit**”.



## Manage Elements

### Elements

[View](#) [Edit](#) [New](#) [Delete](#)

More Actions ▾

Configure Trusted Certificates  
Configure Identity Certificates  
Import

19 Items | [Refresh](#) | Show [ALL](#) ▾

<input type="checkbox"/>	Name ▾	Node	Type	Version	De
<input checked="" type="checkbox"/>	System Manager	localhost	System Manager	6.2	

## Add Trusted Certificate

Select Store Type to add trusted certificate [All](#) ▾

- ☐ Import from existing  
☒ Import from file  
☐ Import as PEM Certificate  
☐ Import using TLS

\* Please select a file  [Browse...](#)

You must click the Retrieve certificate button and review the certificate details before you can continue. [Retrieve Certificate](#)

## 9. User Management

This section describes the details for configuring Converged Users across the Communication Server 1000 and the Collaboration Pack using Element Manager and System Manager User Management.

The Communication Address and Profile Extension number defined for Session Manager and Communication Manager will be a seven-digit number which is identical to corresponding Communication Server 1000 primary Directory Number and the route prefix. In the sample configuration, this would be “2352xx”.

See **Reference [18]** in **Section 12** for more information on bulk importing and synchronizing of existing CS1000 users identities into System Manager.

The following assumes Midsize Enterprise template is configured as the Primary Security Server for the Unified Communications Management application and Communication Server 1000 is registered as a member of the System Manager Security framework.

The following administration steps will be described:

- Confirming users in Communication Server 1000 Element Manager
- Create User Identities and Communication profiles for Session Manager and Communication Manager
- Synchronize Communication Server 1000E Profile to User Identities in System Manager
- Synchronize CallPilot to User Identities in System Manager
- Create User Profile for Messaging (Call Pilot)
- Add PCA and Presence Services to Communication Server 1000E User Communication profiles

**Note:** Some administration screens have been abbreviated for clarity.

### 9.1. Create User Identities and Communication Profiles in System Manager

Communication Server 1000 users have been previously created on Communication Server 1000 Element Manager, with the main endpoint phone TN/DN and CPND (First Name Last Name).

For each Communication Server 1000 user defined in Element Manager a corresponding user identity must be added in System Manager. The **First Name** and **Last Name** of the user must match exactly on both Communication Server 1000 Element Manager and System Manager User Management. This is important for proper Presence synchronization as well as import synchronization for users of their Communication Server 1000 and CallPilot endpoint profile.

Access the web based GUI of Avaya Aura® System Manager by using the URL “**http://<ip-address>/SMGR**”, where **<ip-address>** is the IP address of Avaya Aura® System Manager. Login with the appropriate credentials.

Navigate to **UCM Services - Element Manager – Phone**

Example of a user defined in Element Manager for the sample configuration. Make note of the **First Name** and **Last Name** of the user.

Managing: [EM on cs1knse-cppm\(135.9.139.206\)](#)  
[Phones»Phone Details](#)

## Phone Details



System: EM on cs1knse-cppm  
Phone Type: 1120  
Sync Status: TRN

[General Properties](#) | [Features](#) | [Keys](#) | [User Fields](#)

## General Properties

Customer Number: 0 ★  
Terminal Number: 096 0 00 00

Key No.

Key Type

Key Value

0	SCR - Single Call Ringing	<div> Directory Number: 52001  <input checked="" type="checkbox"/> Multiple Appearance Redirection Prime(MARP)  <div> <div>First Name: Jason</div> <div>Last Name: Giambi</div> <div>Display Format: First, Last</div> <div>Language: Roman</div> </div> </div>
1	NUL - Unassigned	

CLID Entry (Numeric or D): 0  
ANIE Entry:

There are several options for creating user identities in the User Profile Manager (UPM) of System Manager. See **Reference [18] in Section 12** for further information. For the sample configuration, users were manually created in UPM.

To create new users, on the web console for System Manager select **User Management** and then **Manage Users** from left navigation menu.

Click **New** (not shown). Enter values for the following required attributes for a new user in the Identity section and use default values for remaining fields.

- **Last Name:** Enter last name of user.

- **First Name:** Enter first name of user.
- **Login Name:** Enter “**handle**”@<domain>” where “<domain>” matches the domain defined in

### Section 5.1.

- **Authentication Type:** Verify “**Basic**” is selected.
- **Password:** Enter password used to log into System Manager.
- **Confirm Password:** Repeat value entered above.
- **Localized Display Name:** Enter display name for user [Optional].

The screen below shows results from for a new user.

The field names marked with an asterisk (\*) are mandatory fields. Before you click **Commit & Continue** ensure that all the mandatory fields have valid information.

Using the reference configuration, user **Jason Giambi** is created.

Commit & Continue
Com

Identity \*
Communication Profile \*
Membership
Contacts

Identity ▼

\* Last Name:

\* First Name:

Middle Name:

Description:

\* Login Name:

\* Authentication Type: Basic ▼

\* Password:

\* Confirm Password:

Localized Display Name:

Endpoint Display Name:

Title:

Language Preference: English (United States) ▼

Time Zone: (-7:0)Arizona ▼

Employee ID:

Department:

Company:

Next select the **Communication Profile** tab and enter the value the user will use to register to Session Manager in the **Communication Profile Password** and **Confirm Password** fields.

Example: In the reference configuration, “**2352001**” is used as the password.

Verify there is a default entry identified as the **Primary** profile as shown below:

**New User Profile** Commit Cancel

Identity \* **Communication Profile \*** Membership Contacts

Communication Profile ▾

Communication Profile Password:

Confirm Password:

New Delete Done Cancel

Name
Primary

Select : None

\* Name:

Default : ☒

Next, Expand the **Communication Address** sub-section and select **New** to define a **Communication Address** for the new user. Enter values for the following required attributes:

- **Type:** Select “**Avaya SIP**” from drop-down menu.
- **Fully Qualified Address:** Enter same extension number as used for **Login Name** in Step 1.

**Note:** value is shown in **Handle** field after address is added.

- **Domain:** Verify value matches Domain name defined in **Section 4.1**.

Repeat for the following to add Communication Address types **Avaya E.164**.

**Note:** The Avaya XMPP communication address is added automatically to the communication profile because Presence Services is enabled as part of the Avaya Midsize Enterprise template.

Click **Add** (not shown) to save the Communication Address. The screen below shows the results.

**Communication Address** ▾

New Edit Delete

<input type="checkbox"/>	Type	Handle	Domain
<input type="checkbox"/>	Avaya E.164	+2352001	us.global.avaya.com
<input type="checkbox"/>	Avaya SIP	2352001	us.global.avaya.com
<input type="checkbox"/>	Avaya XMPP	jgiambi@pres.ips.avaya.com	




Scroll down to the **Session Manager Profile** section and enter  to expand section.

Enter the following values.

- **Primary Session Manager** Select one of the Session Managers.
- **Origination Application Sequence** Select **Application Sequence** defined for the Communication Manager (drop down available based on ME configuration).
- **Termination Application Sequence** Select **Application Sequence** defined for the Communication Manager drop down available based on ME configuration). Retain the default value of “(None)”.
- **Conference Factory Set** Select “(None)” from drop-down menu.
- **Survivability Server** Select **Location**
- **Home Location**

The screen below shows the results.

☒ **Session Manager Profile** 

\* **Primary Session Manager**

**Secondary Session Manager**

Primary	Secondary	Maximum
13	0	13

Primary	Secondary	Maximum

**Origination Application Sequence**

**Termination Application Sequence**

**Conference Factory Set**

**Survivability Server**

\* **Home Location**

Prior to creating the Communication Manager endpoint profile for each user a customized template is recommended to be created. There is no standard template for Flare Communicator or one-X Mobile based collaboration clients. Using the default 9641 SIP template a duplicate may be made which can then be used for creating the Communication Manager endpoint profiles.

Navigate to **Services – Templates – CM Endpoint**. In the **Endpoint Templates** check the box for **System Type** and **Software Version** as **CM 6.2**.

## Endpoint Templates

### Supported Feature Server Versions

5 Items Refresh Filter: Enable

<input type="checkbox"/>	System Type	Software Version
<input checked="" type="checkbox"/>	CM	6.2
<input type="checkbox"/>	CM	6.0
<input type="checkbox"/>	CM	5.0
<input type="checkbox"/>	CM	5.1
<input type="checkbox"/>	CM	5.2

Select : All, None

In the following screen find the template, “**DEFAULT\_9641SIP\_CM\_6\_2**” and select the checkbox and then select the **Duplicate** button.

Note: Edit and Delete operations are not allowed on Default Templates.

Templates List

View Edit New Duplicate Delete Upgrade

63 Items Refresh Show ALL Filter: Enable

<input type="checkbox"/>	Name	Set Type	Owner	Version	Default	System Type	Software Version	Last Modified
<input type="checkbox"/>	DEFAULT_9641SPCC_CM_6_2	9641SPCC	System	0	Yes	CM	6.2	November 30, 2011 6:46:31 PM - 05:00
<input type="checkbox"/>	DEFAULT_9621SPCC_CM_6_2	9621SPCC	System	0	Yes	CM	6.2	November 30, 2011 6:46:31 PM - 05:00
<input type="checkbox"/>	DEFAULT_9611SPCC_CM_6_2	9611SPCC	System	0	Yes	CM	6.2	November 30, 2011 6:46:00 PM - 05:00
<input type="checkbox"/>	DEFAULT_9608SPCC_CM_6_2	9608SPCC	System	0	Yes	CM	6.2	November 30, 2011 6:46:27 PM - 05:00
<input checked="" type="checkbox"/>	DEFAULT_9641SIP_CM_6_2	9641SIP	System	0	Yes	CM	6.2	November 30, 2011 6:46:28 PM - 05:00
<input type="checkbox"/>	DEFAULT_9621SIP_CM_6_2	9621SIP	System	0	Yes	CM	6.2	November 30, 2011 6:46:08 PM - 05:00
<input type="checkbox"/>	DEFAULT_9611SIP_CM_6_2	9611SIP	System	0	Yes	CM	6.2	November 30, 2011 6:45:39 PM - 05:00

In the next screen, **Duplicate Endpoint Template**, enter in a name for the **New Template Name**, for the reference configuration, “**Flare\_one-X\_SIP**”. Proceed to only check the box for “**IP Softphone**”. Select **Commit** to save the new template.

Home / Services / Templates / CM Endpoint

## Duplicate Endpoint Template

---

Template Name: DEFAULT\_9641SIP\_C

\* Set Type: 9641SIP

System Type: CM

\* New Template Name: Flare\_one-X\_SIP

Software Version: 8.2

---

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)	Button Assignment (B)
Active Station Ringing: single	MWI Served User Type: Select	Per Station CPN - Send Calling Number: Select	IP Phone Group ID:	Remote Soft Phone Emergency Calls: as-on-local	LWC Reception: spe
AUDIX Name:	EC500 State: enabled	Short/Prefixed Registration Allowed: Select	Auto Answer: none	Coverage After Forwarding: system	Display Language: english
			Hunt-to Station:	Loss Group: 19	Survivable COR: internal
			Time of Day Lock Table: Select	Voice Mail Number:	
<b>Features</b> <input type="checkbox"/> Always Use <input type="checkbox"/> IP Audio Hairpinning <input type="checkbox"/> Bridged Call Alerting <input type="checkbox"/> Bridged Idle Line Preference <input checked="" type="checkbox"/> Coverage Message Retrieval			<input type="checkbox"/> Idle Appearance Preference <div style="border: 2px solid red; padding: 2px;"><input checked="" type="checkbox"/> IP SoftPhone</div> <input checked="" type="checkbox"/> LWC Activation <input type="checkbox"/> CDR Privacy <input checked="" type="checkbox"/> Precedence Call Waiting		

Navigate back to **User Management** Users, and then for each user profile:

Scroll down to the **CM Endpoint Profile** section and enter ☒ to expand section.

Enter the following values and use defaults for remaining fields.

- **System** Select Managed Element defined for Communication Manager
- **Profile Type** Select **“Endpoint”**.
- **Use Existing Endpoints** Leave unchecked to automatically create new endpoint when a new user is created.
- **Extension Step 1.** Enter same extension number used for **Login Name** in Step 1.
- **Template** Select the template named **“Flare\_one-X\_SIP”**
- **Security Code** Enter numeric value used to register the SIP endpoint.  
**Note:** this field should match the value entered for the **Communication Profile Password** above, example **“2352001”**
- **Port** Select **“IP”** from drop down menu.
- **Voice Mail Number** Leave field blank.
- **Delete Station on Unassign of Endpoint** Enter ☒ to automatically delete station when **Endpoint Profile** is un-assigned from user [Optional].

The screen below shows the results from above when adding a new SIP user in the reference configuration.

☒ **CM Endpoint Profile** ▼

\* **System** gmi-alphame-cm ▼

\* **Profile Type** Endpoint ▼

**Use Existing Endpoints** ☐

\* **Extension** 2352001 Endpoint Editor

\* **Template** Flare\_one-X\_SIP ▼

**Set Type** 9641SIP

**Security Code**

\* **Port** IP

**Voice Mail Number**

**Preferred Handle** (None) ▼

**Delete Endpoint on Unassign of Endpoint from User or on Delete User** ☒

**Override Endpoint Name** ☒

Select the **Commit & Continue** button (not shown).

## 9.2. Synchronize Communication Profiles

System Manager provides the account synchronization feature to synchronize profile between Communication Server 1000 and CallPilot communication profile and their elements. Using this feature one can synchronize profiles in User Management with the profiles in the respective elements. During synchronization, the account synchronization feature uses the account data in the elements as the master data. Therefore, when a profile data is not in synchronization with the element, the account data from the element is copied to System Manager.

### 9.2.1. Communication Server 1000

This will import and synchronize all Communication Server 1000 users into their previously created System Manager Identity Communication Server 1000 Endpoint Profiles by matching each user (by **Firstname and Lastname**).

Note: A key part of this synchronization is to populate the PSID into each CS1000 user's phone in Element Manager. For the reference configuration example, Jason Giambi, "**jgiambi**", see the screen capture below. The field is cannot be edited manually, only thru the following synchronization process.

Home / Users / User Management / Manage Users

Customer Number:  \*

Terminal Number:

Designation:  \* (1-6 characters)

Zone:  \*

Key Expansion Modules:

[Top](#)

Features

Feature	Description	Value
PSDN	Presence Service DN	<input type="text" value="3000"/>
PUA	Call Pickup	<input type="text" value="Denied"/>
<b>PUID</b>	<b>Presence Unique User ID</b>	<input type="text" value="jgiambi"/>
RBDA	Call Redirection by Day	<input type="text" value="Denied"/>

After building the user identities, perform an on demand synchronization. Navigate to **Elements → Inventory → Synchronization → Communication Server 1000 and CallPilot Synchronization**.

Select the row associated with the Communication Server 1000. Use the **Start** button to initiate the synchronization process. Use the **Refresh** button in the table header to verify status of the synchronization.

Home / Elements / Inventory / CS 1000 and CallPilot Synchronization

**Synchronize Communication Profiles** [Print](#) | [Refresh](#)

Communication Profile Synchronization synchronizes profiles in User Management with profiles in the elements. Select one or more elements, in the list below, and click Start to begin the synchronization process.

**Note:** This process can take a long time to run.

Synchronization Process: Idle

<input type="checkbox"/>	Element ▲	Status	Date	Summary (click to resolve anonymous profiles)
<input checked="" type="checkbox"/>	EM on cs1knse-cppm	PASS	Thu Apr 12 16:20:17 MDT 2012	<a href="#">2 anonymous</a> 1 added 23 profile(s) processed

The above synchronization process will add the **CS 1000 Endpoint Profile** to System Manager for each user name match.

The following is the **CS 1000 Endpoint Profile** for an example for the reference configuration.

☒ **CS 1000 Endpoint Profile**

\* **System**

EM on cs1kns-cppm

\* **Target**

Customer0

\* **Template**

**Service Details**

DN=52001(Marped), TN=096 0 00 00, TYPE=1120

Update

Include in Corporate Directory

☐

## 9.2.2. CallPilot

Next, perform an on demand synchronization to import CallPilot endpoint data to System Manager based on matching user identity data in UPM. Navigate to **Elements → Inventory → Synchronization → Communication Server 1000 and CallPilot Synchronization**.

Select the row associated with the CallPilot. Use the **Start** button to initiate the synchronization process. Use the **Refresh** button in the table header to verify status of the synchronization.

[Home](#) / [Elements](#) / [Inventory](#) / [CS 1000 and CallPilot Synchronization](#)

### Synchronize Communication Profiles

[Print](#) | [Refresh](#)

Communication Profile Synchronization synchronizes profiles in User Management with profiles in the elements. Select one or more elements, in the list below, and click Start to begin the synchronization process.

**Note:** This process can take a long time to run.

Synchronization Process: Idle

Start

Stop

Clear

Reload

<input type="checkbox"/>	Element ▲	Status	Date	Summary (click to resolve anonymous profiles)
1	<input checked="" type="checkbox"/> CallPilot	PASS	Thu Apr 26 12:41:51 MDT 2012	9 updated 9 profile(s) processed

The above synchronization process will add the **CallPilot Endpoint Profile** to System Manager for each user name match.

The following is the **CallPilot Endpoint Profile** for an example for the reference configuration.

## 9.3. Multiple Message Waiting Indication (MWI) for Collaboration

In support of the Converged User, specifically a single voicemail box, the existing CallPilot must be configured to send Message Waiting Indication (MWI) to the Avaya SIP endpoint. For the reference configuration this would be the one of the collaboration clients, one-X Mobile SIP for iOS as the Flare Communicator for iPad does not support MWI at this time.

**Note:** The assumption is the CallPilot mailboxes already exist for each Communication Server 1000 user. If not please refer to **Reference [17] in Section 12**.

To access CallPilot Manager please refer to the respect documentation as listed in the reference above. To enable the MWI for the twinned Avaya one-X Mobile SIP client enter in the **MWI DN #2** as “**2352xx**”, as an example with the reference configuration this would be “**2352001**”. The result is captured in the screen shot below. The user’s twinned Communication Server 1000 client endpoint **MWI DN#1** is “**52001**”

**AVAYA CALLPILOT MANAGER**

LDAP server: bvwcp02 | Mailbox Number: 5080

Home User System Maintenance Messaging Tools Help

Location: User > Add User > Express User Add > Advanced User Add

**Advanced User Add**

Add Cancel Express User Add... Help Times are displayed based on

Advanced Add

Template Name: Regular User Template

Shared Distribution List: None

**General**

First Name\*: Jason

Initial(s):

Last Name\*: Giambi

Comments:

Title:

Department:

**Admin**

Administration Type: No Administration Rights

**Mailbox**

Mailbox Number\*: 52001

Mailbox Class: CallPilot Level 1 [Class Details](#)

Language: English(American)

Location Name: Belleville

Mailbox File System Volume ID: Auto Distribution

Linked to external Directory: Not linked [Link...](#)

**DNs**

Mailbox Shares DN: ☐

Extension DN 1: 52001 ☐ Auto Logon

Extension DN 2:  ☐ Auto Logon

Extension DN 3:  ☐ Auto Logon

Extension DN 4:  ☐ Auto Logon

Extension DN 5:  ☐ Auto Logon

Extension DN 6:  ☐ Auto Logon

Extension DN 7:  ☐ Auto Logon

Extension DN 8:  ☐ Auto Logon

MWI DN1: 52001 ☒ Enabled

MWI DN2: 2352001 ☒ Enabled

## 9.4. Personal Call Assistant Configuration (PCA)

The PCA feature is utilized to enable the twinning of a Communication Server 1000 with an Avaya SIP endpoint (Avaya Aura® Flare Communicator or one-X Mobile Client) so that a “Converged User” may have simultaneous ringing, single number, single voicemail box and aggregated Presence.

To achieve the simultaneous ringing a corresponding PCA must be configured per Converged User. When the Communication Server client endpoint receives an incoming call, the PCA sends call signaling to the Avaya client endpoint via a Communication Server SIP trunk to the Session Manager to effectively “simultaneously ring” the Converged User’s Avaya client endpoint.

The following steps are required to enable this per user, refer to **Reference [6] in Section 12** for further details.

1. Ensure PCA is enabled in the Communication Server 1000 Customer Data Block (not shown).
2. Configure a PCA for every Communication Server 1000 phone user
  - a. The PCA shares the same primary DN on key 0, as the Communication Server 1000 endpoint client.
  - b. Configure key 0 as the Primary DN.
  - c. Configure key 1 as HOT P key, with the AC2 target route prefix and DN as required to reach the twinned Avaya client endpoint.

Navigate to **UCM – Element Manager – Phones**. Search for the **Prime DN** that a PCA is to be added to. For the reference configuration example “**52001**” was used. Next, select the **Add** button.

Managing: EM on cs1knse-oppm(135.9.139.206)  
Search for Phone

---

**Search For Phones**

Criteria: Prime DN Value: 52001

---

Phones Found (2)

Add... Import... Retrieve... Delete <More Actions>

	Customer	TN *	Prime DN	Designation	Phone Type	Te
1	0	096 0.00.00	52001	GMI	1140	

For **Phone Type** select **PCA-Personal Call Assistant** from the drop down menu. Next either enter in the TN or select box (as in this case) to **Automatically assign TN starting TN**. Select the **Preview** button.



## New Phones

Number of phones : 1 \* (1-100)  
Maximum value for Attendant consoles is 63.

Customer : 0

Phone Type: PCA - Personal Call Assistant

Type: ☐ Template ☐ Copy From TN

Options:

- ☐ Default value for DES
- ☐ Default value for ZONE  
Only applicable to IP phone types
- ☐ Default value for Node Id  
Only applicable to UEXT-SIP phone types
- ☒ Automatically assign TN starting TN
- ☐ Automatically assign DN starting DN
- ☐ Automatically assign ACD Position ID starting ACD Position ID
- ☐ Automatically add postfix to SIP User Name starting SIP User Postfix  
Only applicable to UEXT-SIP phone types
- ☐ Automatically assign UADN starting UADN  
Only applicable to UEXT-SIP phone types

\* Required value

Preview Cancel

The following screen will require input to **Customer Number** and **Designation**. For the reference configuration, **Customer Number** is “0” and **Designation** is “Collab”.

## Phone Details

 System: EM on cs1kns-cppm  
Phone Type: PCA  
Syno Status: NEW

General Properties | Features | Keys | User Fields

General Properties

Customer Number: 0 \*

Terminal Number: 098 0 00 02 \*

Designation: Collab \* (1-6 characters)

On the same screen, under **Keys**, for **Key 0** select “MCR-Multiple Call Ringing”, for **Directory Number** enter “52001”, **Key 1** select “Hot\_P-Hotline (PCA)”. The **Target DN Length** is “7” and the **Target DN** is “2352001”.

Keys

Key No.	Key Type	Key Value
0	MCR - Multiple Call Ringing	Directory Number: 62001 <input type="checkbox"/> Multiple Appearance Redirection Prime(MARP) First Name: Jason Last Name: Giambi Display Format: First, Last Language: Roman
1	HOT_P - Hotline(PCA)	CLID Entry (Numeric or D): ANIE Entry: Target DN Length: 7 Target DN: 2352001
2	NUL - Unassigned	
3	NUL - Unassigned	

Select Commit (not shown) to save changes.

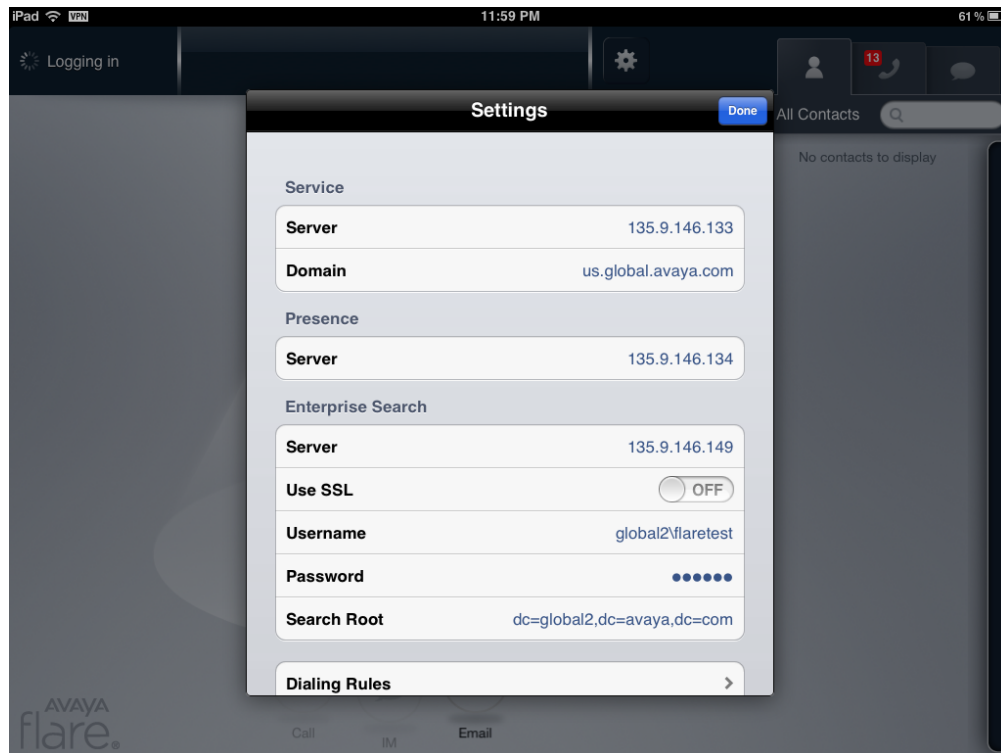
## 9.5. Manual Configuration of Avaya SIP Clients

This section defines the steps to manually configure Avaya Flare Communicator on iPad and Avaya one-X Mobile for SIP iOS running on iPhone/iPod to register to Session Manager.

### 9.5.1. Avaya Flare® Communicator on iPad

Refer to **Reference [19] to [21] in Section 12** on how to obtain, install and configure this client. For the reference configuration, **Server** is the Session Manager asset “**135.9.146.133**” and the Session Manager **Domain** “**us.global.avaya.com**”. For **Presence Server** the IP address is “**135.9.146.134**”.

For the reference configuration the setting for an external LDAP server for the **Enterprise Search Server** is “**135.9.146.149**”. **SSL** is “**OFF**”, **Username** “**global2\flaretest**”, **Password** is “**password**” and **Search Root** is “**dc=global2,dc=avaya,dc=com**”



To login the user must provide the required login credentials, Extension and Password. As an example for the reference configuration, Extension is “**2352001**” and Password “**2352001**”

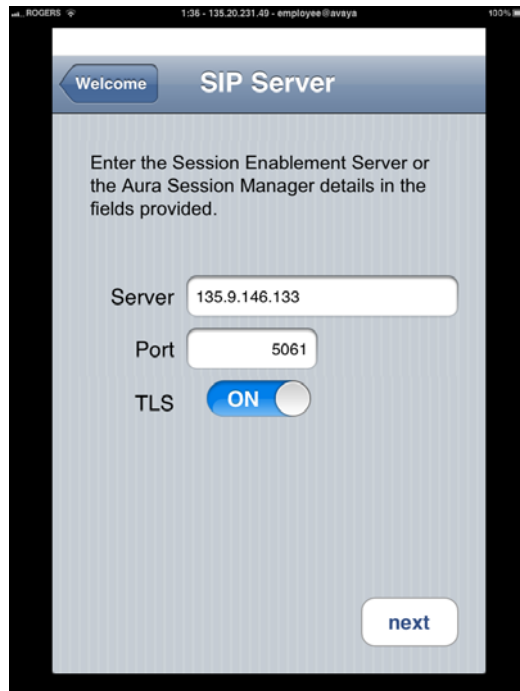


With the login step completed, the user is ready to make and receive calls, watch the Presence of buddies as well as IM with them.

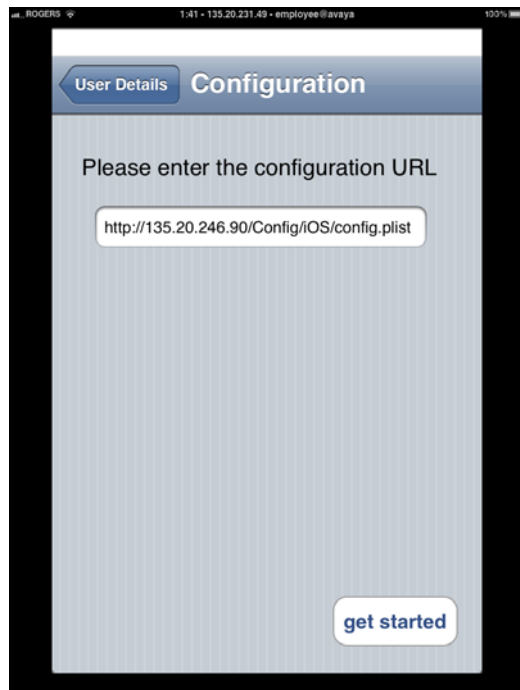
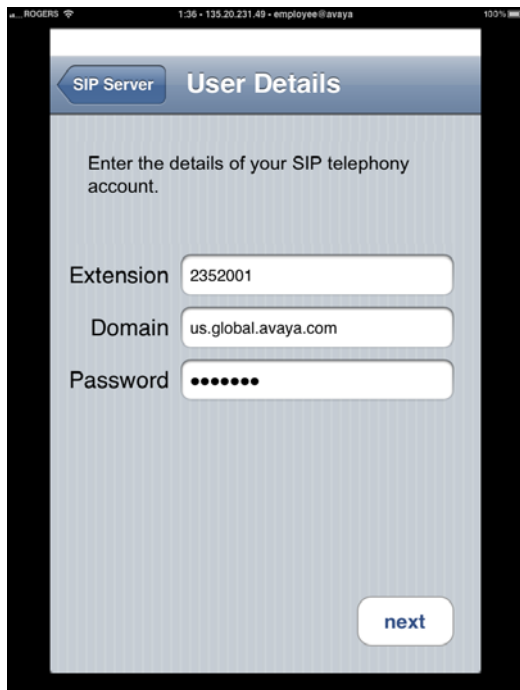


### 9.5.2. Avaya one-X Mobile SIP for iOS on iPhone

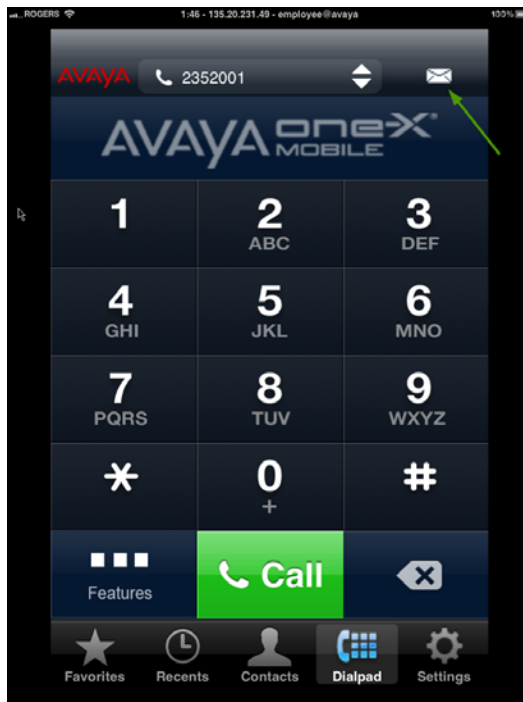
Refer to **Reference [22] and [23] in Section 12** on how to install and configure this client. For the reference configuration, **Server** is the Session Manager asset “**135.9.146.133**”, **TLS** is “**On**”. **Port** is “**5061**”.



The **Extension** for this example reference configuration is “**2352001**” the Session Manager Domain “**us.global.avaya.com**”. The **configuration URL** used was “**http://135.20.246.990/Config/iOS/config.plist**”. Upon completion select the **get started** button.



The screen shot below is a capture of the example reference logged in and the mail icon (MWI) in the upper right hand corner indicating that there is a voicemail for this user.



## 10. Verification Steps

### 10.1. Verify Operational Status

#### 10.1.1. Verify Avaya Aura® Session Manager Operational Status

Navigate to **Elements** → **Session Manager** → **Dashboard** (not shown) to verify the overall system status for Session Manager.

Specifically, verify the status of the following fields as shown below:

- **Tests Pass**
- **Security Module**
- **Service State**

✓  
Up  
Accept New Service

Home / Elements / Session Manager / Dashboard

Help ?

### Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

#### Session Manager Instances

Service State Shutdown System As of 4:03 PM

1 Item | Refresh | Show ALL Filter: Enable

Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	Version
<a href="#">gmi-alpha-sm</a>	Core	0/0/0	✓	Up	Accept New Service	0/5	0	5/7	✓	6.2.0.0.620120

Navigate to **Elements** → **Session Manager** → **System Status** → **Security Module Status** (not shown) to view more detailed status information on the status of Security Module for the specific Session Manager. Verify the **Status** column displays “Up” as shown below.

Home / Elements / Session Manager / System Status / Security Module Status

Help ?

### Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

Reset Synchronize Certificate Management Connection Status

1 Item | Refresh | Show ALL Filter: Enable

Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
<a href="#">Show</a>	<a href="#">gmi-alpha-sm</a>	SM	Up	27	135.9.146.133/24	---	135.9.146.254	Disabled	6/6	Customer CA

### 10.1.2. Verify SIP Entity Link Status

Navigate to **Elements - Session Manager - System Status - SIP Entity Monitoring** (not shown) to view more detailed status information for one of the SIP Entity Links.

Select the each SIP Entity from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page for each SIP entity.

In each of the **All Entity Links to SIP Entity** table for each: **CS1000-Node 1006**, **gmi-alphame-cm** and **gmi-alphame-ps**, verify the **Conn. Status** for the link is “Up” as shown below.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring [Help ?](#)

#### SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

##### All Entity Links to SIP Entity: CS1000-Node1006

Summary View

2 Items | Refresh Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	<a href="#">gmi-alphame-sm</a>	135.9.146.54	5060	TCP	Up	200 OK	Up
► Show	<a href="#">gmi-alphame-sm</a>	135.9.146.54	5061	TLS	Up	200 OK	Up

##### All Entity Links to SIP Entity: gmi-alphame-cm

Summary View

1 Item | Refresh Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	<a href="#">gmi-alphame-sm</a>	135.9.146.130	5060	TCP	Up	200 OK	Up

##### All Entity Links to SIP Entity: gmi-alphame-pres

Summary View

1 Item | Refresh Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	<a href="#">gmi-alphame-sm</a>	135.9.146.134	5061	TLS	Up	400 Missing From URI	Up

### 10.1.3. Verify Registrations of SIP Endpoints

Navigate to **Elements - Session Manager - System Status - User Registrations** to verify the SIP endpoints have successfully registered with both Session Managers.

The screen below shows for the reference configuration the example user **Jason Giambi** is successfully registered with the Session Manager.



## User Registrations

Select rows to send notifications to AST devices. Click on Details column for complete registration status.

AST Device Notifications:    As of 10:54 AM

[Customize](#)

[Advanced Search](#)

17 Items Refresh Show

Filter: Enable

<input type="checkbox"/>	Details	Address	Login Name	First Name	Last Name	Location	IP Address	AST Device	Registered		
									Prim	Sec	Surv
<input type="checkbox"/>	► Show	tholton@us.global.avaya.com		Todd	Holton	Westminster		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	2352001@us.global.avaya.com	jgiambi@us.global.avaya.com	Jason	Giambi	Westminster	135.105.5.89:5061	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	jmoyer@us.global.avaya.com	Jamie	Moyer	Westminster	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 11. Conclusion

This Application Note describes the configuration and test results for the Collaboration Pack initial offer. The Collaboration Pack is made up of the Avaya Aura® Midsize Enterprise solution Release 6.2 and Avaya Communication Server 1000 Release 7.5. The solution enables a traditional Communication Server 1000 client to be twinned with a collaboration client such as the Flare Communicator for iPad and the one-X Mobile – this creates a “Converged User”. This capability provides a Communication Server 1000 user to leverage Unified Collaboration capabilities of the Avaya Aura® Midsize Enterprise solution.

Further Application Notes will be published as additional capabilities are tested and documented with the “Collaboration Pack for CS 1000”.

## 12. Additional References

The following documentation may be obtained from <http://support.avaya.com>.

1. ME Intelligent Workbook
2. Overview of Avaya Aura® Solution for Midsize Enterprise, Release 6.2, Issue 2.2, April 2012
3. Implementing AA solution for Midsize Enterprise Template Release 6.2, Issue 4, April 2012
4. Installation and Upgrades for the Avaya G430 Branch Gateway, Release 6.1, 03-603233, Issue 5, February 2012
5. Network Routing Service Fundamentals Avaya Communication Server 1000, Release 7.5, NN43001-130, 03.10, September 2011
6. IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313,
7. Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116,
8. Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509 Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125,
9. Administering Avaya Aura® Presence Services Release 6.1
10. Administering Avaya Aura® Presence Services XCP Controller
11. Implementing Avaya Aura® Presence Services Release 6.1
12. Presence Services with Communication Server 1000, Document Number NN43001-141, Dec 2011
13. Administering Avaya Aura® Communication Manager, Doc ID 03-300509.
14. Administering Avaya Aura® Communication Manager Server Options, Doc ID 03-603479.
15. Avaya Toll Fraud Security Guide, Doc ID 555-025-600.
16. Avaya Communication Server 1000 and Avaya CallPilot Server Configuration, Document Number NN42300-312
17. Administering Avaya Aura® System Manager, Release 6.2, March 2012.
18. Avaya Flare Overview and Planning Issue 1
19. Administering Avaya Flare Communicator for iPad Devices
20. Implementing Avaya Flare Communicator for iPad Devices
21. Avaya one-X Mobile SIP iOS User Guide
22. Avaya one-X for Apple SIP Clients Administration Guide

## 13. Change History

Issue	Date	Reason
1.0	13/6/2012	Initial issue

---

**©2012 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interoplabinotes@list.avaya.com](mailto:interoplabinotes@list.avaya.com)